

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF NEW YORK**

TIMOTHY O'SULLIVAN,	§
DOMENICK J. ALAGNA, BRIAN	§
CLARK ALLDRIDGE, JOANN	§
ALLDRIDGE, ANDREW CHARLES	§
MAJOR, ASHLEY MEIKEL MAJOR,	§
A.M.M, a minor, RONALD	§
ALLDRIDGE, DIANNA ALLDRIDGE,	§
TODD ALLDRIDGE, CHRISTOPHER	§
B. ANDERSON, TAHNEE	§
ANDERSON, T.A.1, a minor, T.A.2, a	§
minor, K.A., a minor, ERIC J.	§
ATKINSON, TRAVIS R. BASS,	§
HAROLD C. BASS, MARY L.	§
MILTON, ALLEN MILTON, AARON	§
BASS, ADAM C. BASS, LISA	§
LAMBERT, MICHAEL J. BELL,	§
MARK H. BEYERS, DENISE BEYERS,	§
WILLIAM R. BIGGS, DANIEL	§
BIVENS, GRANT R. BLACKWELL,	§
TERAY A. BUNDY, EVAN W.	§
BYLER, GUILLERMO CASTILLO,	§
WILLIAM M. CHINN, WALTER L.	§
THOMAS, THOMAS M. COE II,	§
HEATHER N. COE, V.T.C., a minor,	§
QUENTIN D. COLLINS, MELIDA	§
COLLINS, SIERA N. COLLINS,	§
SHAWN COLLINS, MICHAEL A.	§
COLLINS, I.C.C., a minor, JOSHUA J.	§
COOLEY, CHRISTINE COOLEY, JAY	§
M. FONDREN, ANNE H. FONDREN,	§
M.J.F, a minor, ANTONIO M.	§
FREDERICK, ERNESTO P.	§
HERNANDEZ III, LAURA F.	§
HERNANDEZ, E.H., a minor, N.H., a	§
minor, ERNESTO I HERNANDEZ II,	§
KADE L. HINKHOUSE, JONATHAN	§
B. HOGGE, JOSHUA L. HOLLADAY,	§
SHIRLEY ATKINSON, CRYSTAL	§
HASTINGS, TINA L. HOUGHINS	§
INDIVIDUALLY, AND FOR THE	§
ESTATE OF AARON D. GAUTIER,	§
DANIEL HOUGHINS, PATRICIA A.	§
GAUTIER, ALEXIS HOUGHINS,	§

**PLAINTIFFS' COMPLAINT**

**JURY TRIAL DEMANDED**

**Case No.: \_\_\_\_\_**

GREGORY E. HOGANCAMP, TARA §  
K. HUTCHINSON, JERRALD J. §  
JENSEN, WYMAN H. JONES, IOAN §  
A. KELEMEN, DOUGLAS H. KINARD §  
JR., RANDALL L. KLINGENSMITH, §  
ANGELA KONEN, JONATHAN F. §  
KUNIOLM, MICHELE TERESE §  
QUINN, S.K., a minor, BRUCE §  
KUNIOLM, ELIZABETH §  
KUNIOLM, ERIN KUNIOLM, §  
JOHN MAINE, HARDY P. MILLS IV, §  
CATHY JEAN MILLS, JACOB MILLS, §  
JOSHUA MILLS, JOSEPH C. §  
MIXSON, VIRGINIA B. MIXSON, §  
JOSEPH JOHNSON MIXSON, KARON §  
MIXSON, ALICIA MIXSON, §  
BALTAZAR MORIN JR., MIRANDA §  
A. HARELSTON, JAMES R. §  
NICHOLS, QUEEN NICHOLS, JAMES §  
NICHOLS, THOMAS NICHOLS, §  
SHARON NICHOLS, SEAN M. §  
NIQUETTE, LAUREN NIQUETTE, §  
MELINA ROSE NOLTE §  
INDIVIDUALLY, AND FOR THE §  
ESTATE OF NICHOLAS S. NOLTE, §  
A.N., a minor, ANITA NOLTE, §  
JESSICA NOLTE, JAMES M. OHRT, §  
MICHAEL L. OWEN, LAURIE §  
MILLER, R.O., a minor, COLIN L. §  
PEARCY, LAIRD PEARCY, ANNE §  
PEARCY, JODY STRIKER, KARYN §  
MCDONALD, ANDREW PEARCY, §  
PATRICK PEARCY, ROBERT J. §  
PEARSON, JAMES J. POOLE III, §  
ALLISON P. ROOSIEN, MARK J. §  
PRATT, SONJA RUHREN §  
INDIVIDUALLY, AND FOR THE §  
ESTATE OF DAVID ALAN RUHREN, §  
BRIAN R. SCHAR, BRAD LEE §  
SCHWARZ, DANIEL W. SEGERS, §  
LARRY SEGERS, SHARON W. §  
PARKER, DAVID L. SEGERS, §  
MARTIN SICAIROS, DAVID A. §  
SIMMONS II, KEVIN R. SMITH, §  
JACKAY SMITH, D.S., a minor, L.S., a §  
minor, KAYLA MICHELLE GULLEY, §

ARTHUR B. STOKENBURY, TRAVIS §  
M. STRONG, TAYLER HESTON, §  
ANTHONY J. DURKACS, KOMA K. §  
TEXEIRA, BRIMA TURAY, RUTH §  
TURAY, ALLEN R. VAUGHT, §  
GRANT BLANEY VON LETKEMANN §  
II, KELLY LYNN VON LETKEMANN, §  
ANTONIO H. WARD, DENNIS §  
WARD, DALLAS WARD, GEORGE L. §  
WILLIAMS, ELIZABETH G. §  
WILLIAMS, KAYLEIGH A. §  
WILLIAMS, NICKOLAS A. §  
WILLIAMS, SEAN LEE WILLIAMS, §  
SUE ANN WILLIAMS, JOSHUA B. §  
WOLFE, JEFF M. WRIGHT, ROGER L. §  
YOUNG, §  
§

Plaintiffs, §  
§

vs. §  
§

DEUTSCHE BANK AG; HSBC BANK §  
USA, N.A.; HSBC HOLDINGS Plc; §  
HSBC BANK Plc; HSBC BANK §  
MIDDLE EAST LIMITED; HSBC §  
NORTH AMERICA HOLDINGS, INC.; §  
COMMERZBANK AG; §  
COMMERZBANK AG, NEW YORK §  
BRANCH; BARCLAYS BANK Plc; §  
BNP PARIBAS S.A.; STANDARD §  
CHARTERED BANK; ROYAL BANK §  
OF SCOTLAND N.V.; ROYAL BANK §  
OF SCOTLAND PLC; CRÉDIT §  
AGRICOLE S.A.; CRÉDIT AGRICOLE §  
CORPORATE & INVESTMENT §  
BANK; CREDIT SUISSE AG; and §  
BANK SADERAT Plc, §  
§

Defendants. §  
§  
§  
§

## TABLE OF CONTENTS

I.	INTRODUCTION .....	1
II.	JURISDICTION AND VENUE .....	12
	A.    This Court Has Jurisdiction Over All Claims and All Parties. ....	12
	1.    Subject Matter Jurisdiction .....	12
	2.    Personal Jurisdiction .....	12
	B.    Venue is Proper in this Court.....	16
III.	THE PLAINTIFFS & THE TERRORIST ATTACKS .....	16
	A.    The March 2, 2008 Attack – Basra .....	18
	1.    Plaintiff Timothy Joseph O’Sullivan .....	18
	B.    The October 12, 2011 Attack – COS Gary Owen .....	19
	1.    Plaintiffs The Alldridge Family .....	19
	C.    The July 10, 2011 Attack – Forward Operating Base Garry Owen.....	21
	1.    Plaintiffs The Niquette Family.....	21
	2.    Plaintiff William M. Chinn .....	22
	D.    The June 6, 2011 Attack – Camp Loyalty .....	22
	1.    Plaintiff Walter Leman Thomas.....	22
	E.    The February 16, 2011 Attack—Route Tomatoes, Baghdad, Near Sadr City.....	23
	1.    Plaintiff Walter Leman Thomas.....	23
	F.    The November 20, 2009 Attack – Supply Route of Kalzoo .....	24
	1.    Plaintiffs The Holladay Family.....	24
	G.    The August 21, 2009 Attack – Route Irish, Baghdad.....	25
	1.    Plaintiff Randall Lavis Klingensmith .....	25
	H.    The November 22, 2008 Attack –En Route to FOB Kalsu.....	25
	1.    Plaintiffs The Owen Family.....	25

2.	Plaintiffs The Williams Family.....	27
I.	The August 8, 2008 Attack – Baghdad.....	28
1.	Plaintiffs The Morin/Harelston Family.....	28
J.	The April 28, 2008 Attack – FOB Loyalty .....	29
1.	Plaintiffs The Coe Family.....	29
K.	The April 13, 2008 Attack – Sadr City .....	30
1.	Plaintiff Michael James Bell.....	30
L.	The April 8, 2008 Attack – MSR Tampa.....	30
1.	Plaintiffs The Collins Family.....	30
M.	The April 4, 2008 Attack – Victory Base Complex, Baghdad .....	32
1.	Plaintiffs The Von Letkemann Family .....	32
N.	The March 26, 2008 Attack – FOB Phoenix .....	33
1.	Plaintiffs The Hernandez Family .....	33
O.	The November 2, 2007 Attack – Route Senators Highway, Baghdad.....	34
1.	Plaintiffs The Poole Family .....	34
P.	The October 31, 2007 Attack – Sadr City, Baghdad .....	35
1.	Plaintiff Koma Kekoa Texeira .....	35
Q.	The September 29, 2007 Attack - Baghdad.....	36
1.	Plaintiff Eric James Atkinson .....	36
R.	The September 19, 2007 Attack – Kadhimiyah.....	36
1.	Plaintiff Brian Robert Schar.....	36
S.	The September 4, 2007 Attack – Sadar City, Baghdad .....	37
1.	Plaintiffs The Mixson Family .....	37
T.	The August 22, 2007 Attack – Baghdad/Sadr City Border .....	38
1.	Plaintiff Jerrald J. Jensen .....	38

U.	The July 17, 2007 Attack – Sadr City .....	39
1.	Plaintiffs The Pearcy Family .....	39
V.	The July 11, 2007 Attack – Forward Operating Base Hammer.....	40
1.	Plaintiffs The Smith Family.....	40
W.	The July 10, 2007 Attack – Observation Point Cavalier, Taji .....	41
1.	Plaintiffs The Segers Family.....	41
X.	The June 17, 2007 Attack – Basra .....	42
1.	Plaintiff Grant Ransom Blackwell .....	42
Y.	The May 31, 2007 Attack - Baghdad.....	43
1.	Plaintiff John Maine.....	43
Z.	The May 28, 2007 Attack – Sadr City .....	44
1.	Plaintiff Gregory Edward Hogancamp .....	44
AA.	The May 17, 2007 Attack – Baghdad .....	44
1.	Plaintiffs The Gautier/Houchins Family .....	44
BB.	The April 27, 2007 Attack – Fallujah, Iraq.....	46
1.	Plaintiff Guillermo Castillo.....	46
CC.	The February 25, 2007 Attack – CSC Scania .....	46
1.	Plaintiff Joshua Bradley Wolfe.....	46
DD.	The February 3, 2007 Attack – Route Dover, South of Camp Taji .....	47
1.	Plaintiffs The Bass Family.....	47
EE.	The January 27, 2007 Attack – Route Michigan, Baghdad .....	48
1.	Plaintiffs The Nichols Family .....	48
FF.	The December 19, 2006 Attack - Ramadi .....	49
1.	Plaintiff William Robert Biggs .....	49
GG.	The November 27, 2006 Attack – Shula.....	50

1.	Plaintiffs The Strong Family.....	50
HH.	The February 14, 2006 Attack – Baghdad.....	51
1.	Plaintiff Tara Kathleen Hutchinson .....	51
II.	The October 26, 2005 Attack – Dunbar Province.....	52
1.	Plaintiff Martin Sicairos.....	52
JJ.	The October 8, 2005 Attack – Ramadi, Iraq.....	52
1.	Plaintiff Kade Luther Hinkhouse .....	52
KK.	The September 2, 2005 Attack - Mosul.....	53
1.	Plaintiff Ioan Adrian Kelemen.....	53
LL.	The August 26, 2005 Attack – Hit, Iraq.....	54
1.	Plaintiffs The Beyers Family .....	54
MM.	The August 13, 2005 Attack – Sadr City, Iraq .....	54
1.	Plaintiff Brad Lee Schwarz.....	54
NN.	The July 5, 2005 Attack – Hit, Iraq .....	55
1.	Plaintiffs The Cooley Family .....	55
OO.	The April 19, 2005 Attack – Route Midland .....	56
1.	Plaintiff Antonio Martinez Frederick.....	56
PP.	The April 18, 2005 Attack – Karbala.....	57
1.	Plaintiff Wyman Harrell Jones.....	57
QQ.	The March 15, 2005 Attack - Baghdad.....	57
1.	Plaintiff Douglas Hamilton Kinard Jr.....	57
RR.	The January 1, 2005 Attack – Haditha.....	58
1.	Plaintiffs The Kuniholm Family .....	58
SS.	The December 21, 2004 Attack – FOB Marez, Mosul .....	59
1.	Plaintiffs The Ruhren Family.....	60

2.	Plaintiff Mark Joseph Pratt .....	61
3.	Plaintiff Evan Wayne Byler .....	61
4.	Plaintiff Teray Anton Bundy .....	62
5.	Plaintiff Jeff McKinley Wright.....	62
6.	Plaintiffs The Turay Family.....	63
7.	Plaintiff Daniel Bivens.....	63
8.	Plaintiff Eric James Atkinson .....	64
9.	Plaintiff Angela Konen .....	64
10.	Plaintiff Jonathan B. Hogge.....	65
11.	Plaintiff James Michael Ohrt .....	65
12.	Plaintiffs The Williams Family.....	65
13.	Plaintiffs The Ward Family .....	66
14.	The Anderson Family .....	67
15.	Plaintiffs The Collins Family.....	68
TT.	The November 24, 2004 Attack - Baghdad .....	70
1.	Plaintiffs The Fondren Family .....	70
UU.	The November 9, 2004 Attack – Iskandariya .....	71
1.	Plaintiffs The Nolte Family .....	71
VV.	The October 31, 2004 Attack – FOB Marez, Mosul, Iraq .....	72
1.	Plaintiff Jonathan B. Hogge .....	72
WW.	The August 16, 2004 Attack – Sadr City, Baghdad.....	73
1.	Plaintiff David Allen Simmons II .....	73
XX.	The June 29, 2004 Attack – Camp Fallujah.....	74
1.	Plaintiffs The Mills Family .....	74
YY.	The June 21, 2004 Attack – Combat Outpost Apache.....	75

1.	Plaintiff Arthur B. Stokenbury.....	75
ZZ.	The April 9, 2004 Attack – Market area of Baiji.....	75
1.	Plaintiff Domenick Jared Alagna.....	75
AAA.	The March 13, 2004 Attack – Karbala.....	76
1.	Plaintiff Robert James Pearson .....	76
BBB.	The December 23, 2003 Attack – Sadr City, Baghdad.....	77
1.	Plaintiff Roger Lee Young.....	77
CCC.	The December 17, 2003 Attack – Sadr City .....	78
1.	Plaintiff Allen Ryan Vaught .....	78
IV.	<b>ALL OF THE TERRORIST ATTACKS WERE ACTS OF INTERNATIONAL TERRORISM.....</b>	79
A.	The Acts committed by the Terrorist Groups and Defendants referenced in the complaint were acts of international terrorism pursuant to 18 U.S.C. § 2331 et. seq. ....	79
B.	The United States was not engaged in a war or armed conflict with Iran during the Relevant Period.....	80
C.	The invasion of Iraq was authorized by United Nations Resolutions under Chapter VII of the U.N. Charter.....	81
D.	Prior to June 20, 2004, all U.S. forces and civilians were present in Iraq in accordance with international law with the goal to restore full sovereignty to the Iraqi people. ....	82
E.	U.S. forces were present in Iraq subsequent to June 19, 2004, at the invitation of the government of Iraq and pursuant to a mandate by the United Nations.....	84
F.	The Terrorist Groups were not “military forces” under 18 U.S.C. § 2331 et. Seq. ....	85
G.	The attacks perpetrated by the Terrorist Groups were criminal acts of international terrorism and not legitimate attacks by military forces during an armed conflict.87	87
H.	Hezbollah .....	92
I.	Al Qaeda .....	96
J.	Ansar al Sunna/Ansar al Islam.....	100

K.	Jaysch al Mahdi.....	101
L.	Badr Organization.....	102
M.	Kata'ib Hezbollah .....	104
N.	Asa'ib Ahl al-Haq.....	106
V.	THE DEFENDANTS.....	106
A.	Deutsche Bank AG .....	110
B.	The HSBC Defendants.....	111
1.	HSBC Holdings Plc .....	114
2.	HSBC North America Holdings, Inc. ....	114
3.	HSBC Bank USA, N.A.....	115
4.	HSBC Bank Plc .....	116
5.	HSBC Bank Middle East Limited.....	116
C.	Commerzbank AG and Commerzbank AG, New York Branch.....	117
D.	Barclays Bank Plc.....	117
E.	BNP Paribas S.A.....	118
F.	Standard Chartered Bank .....	119
G.	Royal Bank of Scotland N.V. and Royal Bank of Scotland Plc .....	120
H.	Crédit Agricole S.A. and Crédit Agricole Corporate & Investment Bank .....	122
I.	Credit Suisse AG.....	124
J.	Bank Saderat Plc .....	127
VI.	FACTUAL ALLEGATIONS .....	130
A.	Islamic Republic of Iran a/k/a Iran .....	130
1.	Iran Finances and Supports Terrorism and Terrorist Organizations.....	130
2.	Economic Sanctions were Implemented to Stop Iran from Sponsoring Terrorism.....	132
3.	Need for the Conspiracy .....	134

4.	Who Best to Conspire With .....	135
5.	Defendants Were Warned Not To, But They Did It Anyway.....	135
6.	Effect of Defendants' actions on Iran's Economy .....	136
7.	Iran's Long History of Materially Supporting And Encouraging Acts of International Terrorism .....	138
8.	Iran's Sponsorship and Material Support of Terrorism in Iraq.....	142
9.	Islamic Revolutionary Guard Corps .....	144
10.	Islamic Revolutionary Guard Corps-Qods Force .....	146
11.	Hezbollah .....	148
12.	Iran's Ministry of Defense and Armed Forces Logistics.....	150
13.	The Iranian Ministry of Intelligence and Security .....	152
B.	Iran's Terrorist Network in Iraq.....	156
1.	Ansar al Islam / Ansar al Sunna.....	156
2.	Special Groups .....	161
3.	The Badr Corps/Badr Organization .....	165
4.	Kata'ib Hizbollah.....	166
5.	Jaysch al Mahdi and The Promised Day Brigades.....	171
6.	Asa'ib Ahl Al-Haq.....	173
7.	Al Qaeda .....	174
8.	Abu Musab Zarqawi .....	182
C.	Iranian Signature Weapons Used in the Terrorist Attacks.....	187
1.	Explosively Formed Penetrators .....	187
2.	Improvised Rocket Assisted Munitions .....	192
D.	Iran Evades Sanctions Through Its Agents/Proxies.....	194
1.	Bank Markazi Jomhouri Islami Iran .....	195
2.	Bank Melli Iran and Melli Bank Plc .....	196

3.	Bank Mellat.....	199
4.	Bank Sepah .....	202
5.	Islamic Republic of Iran Shipping Lines .....	204
6.	National Iranian Oil Company.....	209
7.	Mahan Air .....	211
8.	Khatam al-Anbiya Construction Company & The Headquarters for the Restoration of Holy Shrines.....	213
E.	Iran's Need for U.S. Dollars .....	221
F.	The U.S. Sanctions on Iran .....	223
1.	Sanctions Under the International Emergency Economic Powers Act...	224
a.	Executive Order 12957 .....	224
b.	Executive Order 13224 .....	226
2.	Iran Evades Sanctions .....	228
3.	The U.S. Financial System as a Frontline Defense.....	229
VII.	THE CONSPIRACY .....	230
A.	Perpetrating the Conspiracy .....	238
1.	Stripping Wire Transfer Information .....	240
2.	Non-Transparent Cover Payments.....	241
3.	U-Turns .....	242
4.	Trade Finance.....	244
B.	Defendants' Agreement to, and Participation in, the Conspiracy.....	247
1.	Defendants Had a Duty to Ensure Their Acts Did Not Fund Terrorist Organizations and Knew of that Duty .....	247
2.	Deutsche Bank AG's Participation in the Conspiracy .....	257
3.	The HSBC Defendants' Participation in the Conspiracy.....	269
4.	Commerzbank's Participation in the Conspiracy .....	299

5.	Barclays' Participation in the Conspiracy.....	319
6.	BNP's Participation in the Conspiracy .....	332
7.	Standard Chartered Bank's Participation in the Conspiracy.....	354
8.	RBS' Participation in the Conspiracy .....	399
9.	Crédit Agricole's Participation in the Conspiracy.....	418
10.	Credit Suisse's Participation in the Conspiracy.....	438
C.	Defendant Bank Saderat's and Iranian Bank Co-Conspirators' Agreement to, and Participation in, the Conspiracy.....	458
D.	Defendants Knowingly Provided Iran with U.S. Dollars, Thereby Allowing Iran to Fund the Terrorist Attacks That Killed or Injured Plaintiffs .....	471
VIII.	THE ACTS OF DEFENDANTS CAUSED PLAINTIFFS' INJURIES AND DEATHS .....	473
IX.	CLAIMS FOR RELIEF .....	474
A.	First Claim for Relief: Primary Liability Under 18 U.S.C. § 2333(a) Against All Defendants for Providing Material Support to Terrorist Groups in Violation of 18 U.S.C. § 2339A.....	474
B.	Second Claim for Relief: Primary Liability Under 18 U.S.C. § 2333(a) Against Commerzbank For Providing Material Support to Terrorists in Violation of 18 U.S.C. § 2339A .....	483
C.	Third Claim for Relief: Primary Liability Under 18 U.S.C. § 2333(a) Against Standard Chartered Bank for Providing Material Support to Terrorists in Violation of 18 U.S.C. § 2339A.....	485
D.	Fourth Claim for Relief: Primary Liability Under 18 U.S.C. § 2333(a) Against Commerzbank AG for Providing Material Support to Hezbollah in Violation of 18 U.S.C. § 2339B .....	488
E.	Fifth Claim for Relief: Secondary Liability Under 18 U.S.C. § 2333(a) Against All Defendants for Participating in the Conspiracy .....	489
F.	Sixth Claim for Relief: Secondary Liability Under 18 U.S.C. § 2333(a) Against Commerzbank AG for Aiding and Abetting Hezbollah, a Designated Foreign Terrorist Organization.....	494
G.	Seventh Claim for Relief: Secondary Liability Under 18 U.S.C. § 2333(a) Against All Defendants for Aiding and Abetting an Act of International Terrorism	

Committed, Planned, or Authorized by Designated Foreign Terrorist Organizations .....	497
H. Eighth Claim for Relief: Primary Liability Against HSBC Bank USA, N.A. Under 18 U.S.C. § 2333(a) for Engaging in Financial Transactions with Iran in Violation of 18 U.S.C. § 2332d .....	503
I. Ninth Claim for Relief: Primary Liability Under 18 U.S.C. § 2333(a) Against Standard Chartered Bank, Royal Bank of Scotland N.V., Commerzbank, Deutsche Bank AG, Barclays Bank Plc, and Credit Suisse, for Engaging in Financial Transactions with Iran and its Agents and Proxies in Violation of 18 U.S.C. § 2332d.....	506
J. Tenth Claim for Relief: Primary Liability Under 18 U.S.C. § 2333(a) Against BNP for Engaging in Financial Transactions with Iran and Sudan and Their Agents and Proxies in Violation of 18 U.S.C. § 2332d .....	510
X. PRAYER FOR RELIEF .....	514

## INDEX OF ACRONYMS

**AAH** – Asa’ib Ahl Al Haq or the “League of the Righteous”

**AAI** – Ansar al Islam

**AIO** – Aerospace Industries Organization

**AML** – Anti-money laundering

**AO** – Area of Operation

**ATA** – Anti-terrorism Act, 18 U.S.C. § 2333, *et seq.*

**BIC** – Bank Identifier Code

**BNP** – BNP Paribas S.A.

**BSA** - Bank Secrecy Act

**CACIB** – Crédit Agricole Corporate and Investment Bank

**CAIS** - Crédit Agricole Indosuez (Suisse)

**CASA** - Crédit Agricole S.A.

**CBI** – Central Bank of Iran

**CHIPS-NY** – Clearing House Interbank Payment System

**CIF** – Customer Information File

**CL** – Crédit Lyonnais

**CLS** – Credit Lyonnais (Suisse) S.A.

**CSAM** – Credit Suisse Asset Management Limited, United Kingdom

**DB** – Deutsche Bank AG

**DFAC** – Dining Facility

**DFS** – Department of Financial Services

**DIO** – Defense Industries Organization

**DN** – Specially Designated Nation

**DOJ** - Department of Justice

**DPA** – Deferred Prosecution Agreement

**EFP** – Explosively formed penetrators

**FATF** – Financial Action Task Force

**FinCEN** – Financial Crimes Enforcement Network

**FINMA** – The Swiss Financial Market Supervisory Authority

**FOB** – Forward Operating Base

**FRBNY** – Federal Reserve Board of New York

**FTO** – Foreign Terrorist Organization

**HBEU** – HSBC Bank Plc aka HSBC-London

**HBME** – HSBC Middle East Limited aka HSBC-Middle East

**HSBC-US** – HSBC Bank USA, N.A.

**HRHS** – The Headquarters for the Restoration of Holy Shrines

**IAMIC** – Iran Aircraft Manufacturing Industrial Company aka HESA

**ICC Statute** – Rome Statute of the International Criminal Court

**ICEI** - Imensazen Consultant Engineers Institute

**IED** – Improvised explosive device

**IEEPA** – International Emergency Economic Powers Act

**IHL** – International Humanitarian Law

**IHRL** – International Human Rights Law

**IHSRC** – Iran Helicopter Support and Renewal Company aka PAHNA

**IOVB** – Bank Saderat in London

**IRAM** – Improvised Rocket Assisted Munitions

**IRGC** – Islamic Revolutionary Guard Corps

**IRGC-QF** – Islamic Revolutionary Guard Corps-Qods Force

**IRISL** – Islamic Republic of Iran Shipping Lines

**ISIL** – Islamic State of Iraq and the Levant aka “ISIS” or “Daesh”

**ITR** – Iranian Transactions Regulations

**ITRSHRA** – Iran Threat Reduction and Syrian Human Rights Act of 2012

**JAM** – Jaysch al Mahdi or the “Mahdi Army”

**JASTA** – Justice Against Sponsors of Terrorism Act, Pub. L. 114-222, Sept. 28, 2016, 130 Stat. 852

**KAA** - Khatam al-Anbiya Construction Company (a/k/a Khatam al-Anbiya Construction Headquarters, Qaragah-e Sazandegi-ye Khatam al-Anbiya, or “Seal of the Prophets”)

**KH** – Kata’ib Hizballah

**LC** – Letter of Credit

**MNF-I** – Multi National Forces in Iraq

**MODAFL** – Iran’s Ministry of Defense and Armed Forces Logistics

**MOIN** – Monitoring and Investigations Unit

**MOIS** – Iran’s Ministry of Intelligence and Security

**MPD** – Multicurrency Payments Department

**MT** – Message Type

**NIOC** – National Iranian Oil Company

**NSN** – National Stock Number

**OFAC** – U.S. Department of Treasury Office of Foreign Asset Control

**OPEC** - Organization of Petroleum Exporting Countries

**PAHNA** – *See* IHSRC

**PCM** – Payment and Cash Management

**PDB** – Promised Day Brigades

**RBS Plc** – The Royal Bank of Scotland Plc

**RBS Group** – The Royal Bank of Scotland Group Plc

**RBS N.V.** – The Royal Bank of Scotland N.V.

**SCB** – Standard Chartered Bank

**SDGT** – Specially Designated Global Terrorist

**SDN** – Specially Designated National

**SDT** – Specially Designated Terrorist

**SWIFT** – Society for Worldwide Interbank Financial Telecommunication

**TBI** – Traumatic Brain Injury

**UAE** – United Arab Emirates

**UBL** – Usama bin Laden

**USD** – United States Dollars

**VBIED** – Vehicle-Borne Improvised Explosive Device a/k/a car bomb

**WMD** – Weapons of Mass Destruction

## I. INTRODUCTION

1. “[M]oney is the oxygen of terrorism,” as Secretary of State Colin Powell observed. “Without the means to raise and move money around the world, terrorists cannot function.”

2. This case is about the corporate greed of certain multinational banks (the named Defendants) and the resulting deaths and serious injuries to hundreds of U.S. nationals<sup>1</sup> in Iraq due to acts of international terrorism.

3. In what is perhaps one of the most egregious instances of placing profits over people, Defendants<sup>2</sup> used the U.S. banking system, in concert with Defendant Bank Saderat Plc<sup>3</sup> (“Bank Saderat”), Iran, and its Agents and Proxies,<sup>4</sup> to deliberately evade economic sanctions against Iran—sanctions put in place with the singular goal of stopping Iran, the world’s leading state sponsor of terrorism, from sponsoring terrorism.

---

<sup>1</sup> As used in the Complaint, the terms “United States’ nationals,” “nationals of the United States,” and “U.S. nationals” have the meaning set forth in the Immigration and Nationality Act, codified at 8 U.S.C. § 1101(a)(22), which defines the term “national of the United States” as “. . . (A) a citizen of the United States, or (B) a person who, though not a citizen of the United States, owes permanent allegiance to the United States.”

<sup>2</sup> Defendants are (1) Deutsche Bank AG; (2) HSBC Bank USA, N.A.; (3) HSBC Holdings Plc; (4) HSBC Bank Plc; (5) HSBC Bank Middle East Limited; (6) HSBC North America Holdings, Inc.; (7) Commerzbank AG; (8) Commerzbank AG, New York Branch; (9) Barclays Bank Plc; (10) BNP Paribas S.A.; (11) Standard Chartered Bank; (12) Royal Bank of Scotland N.V.; (13) Royal Bank of Scotland Plc (14) Crédit Agricole S.A.; (15) Crédit Agricole Corporate & Investment Bank; and (16) Credit Suisse A.G.

<sup>3</sup> According to the Treasury Department, Tehran used Bank Saderat to channel funds to U.S. - designated terrorist organizations, including Hezbollah, Hamas, the Popular Front for the Liberation of Palestine-General Command, and Palestinian Islamic Jihad. *See Avi Jorisch, IRAN’S DIRTY BANKING – HOW THE ISLAMIC REPUBLIC SKIRTS INTERNATIONAL FINANCIAL SANCTIONS* 3 (2010).

<sup>4</sup> Iran’s Agents and Proxies include the individuals and entities listed on the United States Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) Sanctions Lists including, but not limited to: (1) Bank Markazi Jomhouri Islami Iran (“Bank Markazi”) (a/k/a the “Central Bank of the Islamic Republic of Iran”); (2) Bank Melli Iran; (3) Melli Bank Plc; (4) Bank Mellat; (5) Bank Tejarat; (6) Bank Refah; (7) Bank Sepah; (8) Bank Saderat Plc; (9) the IRISL; (10) Mahan Air; (11) Iran Air; (12) the state owned and operated National Iranian Oil Company (“NIOC”); (13) the Islamic Revolutionary Guard Corps (“IRGC”); (14) Islamic Revolutionary Guard Corps-Qods Force (“IRGC-QF”); (15) Khatam-al Anbiya Construction; and (16) the Terrorist Groups. Pursuant to 31 C.F.R. § 560.304, Bank Markazi, Bank Sepah, Bank Melli, and the NIOC are considered part of the government of Iran.

4. The purpose of evading these sanctions was to launder money for Iran's Agents and Proxies (and ultimately for the Terrorist Groups), as well as to obstruct law enforcement from cutting off the flow of United States dollars ("USDs") to Iran, sanctioned entities, and terrorists. Defendants knew, or were deliberately indifferent to the fact, that such USDs provided material support to Terrorist Groups<sup>5</sup> thereby enabling them to commit heinous acts of violence against United States nationals, including Plaintiffs.

5. Lest there be any doubt about Defendants' contempt for the sanctions and related banking regulations that were designed to stop Iran's sponsorship of terrorism, one need only read the response by Standard Chartered Bank Group's Executive Director to an October 2006 email from Standard Chartered's CEO.

6. The CEO wrote, "we believe [the Iranian business] needs urgent reviewing at the Group level to evaluate if its returns and strategic benefits are . . . still commensurate with the potential to cause *very serious or even catastrophic reputational damage to the Group...* [T]here is equally important potential of risk of subjecting management in US and London (e.g. you and I) and elsewhere to personal reputational damages and/or *serious criminal liability*."<sup>6</sup>

---

<sup>5</sup> As used herein, the term "Terrorist Groups" refers to Hezbollah (designated a Foreign Terrorist Organization "FTO" on October 8, 1997), al Qaeda, (designated an FTO on October 8, 1999), all al Qaeda subgroups, (including al Qaeda in Iraq, which was designated an FTO on December 17, 2004), Ansar al Islam/Ansar al Sunna (designated an FTO on March 22, 2004)), the Special Groups (including Jayesch al Mehdi, Badr Organization/Badr Brigades, Kata'ib Hizballah (designated an FTO on July 2, 2009), Asa'ib Ahl al Haq, Promised Day Brigades, Abu Mustafa Al-Sheibani network, Abu Mahdi al-Muhandis network, and others discussed at Section VI.B.2. below), Foreign Terrorist Organizations, Specially Designated Global Terrorists, Specially Designated Terrorists, and/or Specially Designated Nationals, IRGC-QF and other terrorists, which were responsible for the Terrorist Attacks..

<sup>6</sup> Memorandum entitled *Business with Iran – USA Perspective* by SCB's CEO, Americas to SCB's Group Executive Director for Risk, its Group Head of Public Affairs dated October 5, 2006, SCB INT 0005759-5762 (emphasis added).

7. The Group Director's response was: "**You f---ing Americans. Who are you to tell us, the rest of the world, that we're not going to deal with Iranians.**"<sup>7</sup>

8. On October 13, 2017, in an official White House statement, President Donald J. Trump stated, "In Iraq and Afghanistan, groups supported by Iran have killed hundreds of American military personnel. The Iranian dictatorship's aggression continues to this day. The regime remains the world's leading state sponsor of terrorism, and provides assistance to al Qaeda, the Taliban, Hezbollah, Hamas, and other terrorist networks. It develops, deploys, and proliferates missiles that threaten American troops and our allies. It harasses American ships and threatens freedom of navigation in the Arabian Gulf and in the Red Sea. It imprisons Americans on false charges. And it launches cyberattacks against our critical infrastructure, financial system, and military."

9. This is a civil action pursuant to the Anti-Terrorism Act (18 U.S.C. § 2331, *et seq.*) (hereinafter "ATA") and the Justice Against Sponsors of Terrorism Act (Pub. L. 114-222, Sept. 28, 2016, 130 Stat. 852) ("JASTA").

10. JASTA was enacted by Congress "to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against persons, entities, and foreign countries, wherever acting and wherever they may be found, that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States."

---

<sup>7</sup> Note of Interview with SCB's Head of Cash Management Services (2002-2005), Head of Compliance (2005-2007) at the New York branch, SCB INT 0004733-4734.

11. This action is brought on behalf of nationals of the United States (as well as their family members) who were serving as members of the U.S. armed forces at the time they were injured or killed by the Terrorist Groups in Iraq from 2003 to 2011 (the “Relevant Period”).

12. Plaintiffs were killed or injured by acts of international terrorism while serving in Iraq and assisting in the peacekeeping mission designed to stabilize the country and establish a free and democratic government.

13. On January 19, 1984, the United States designated Iran a State Sponsor of Terrorism. Such a designation is made by the U.S. Secretary of State, who must first determine the government in question has repeatedly provided support for acts of international terrorism. Iran’s designation is still in force. Indeed, since 1984, Iran has been the world’s leading state sponsor of terror.

14. Iran, through its Agents and Proxies (including the Terrorist Groups), especially Hezbollah<sup>8</sup> (a militant group that was created by the Iranian military in the early 1980s to further Iran’s political objectives abroad), has been actively involved in supporting and promoting terrorism in Iraq since before the U.S. invasion in 2003.

15. Since then, Iran continually supplied weapons and training to insurgent groups, both Sunni and Shia, in Iraq and supported the groups as they targeted Coalition Forces,<sup>9</sup> Iraqi security forces, and the Iraqi government itself.

---

<sup>8</sup> The pronunciation and spelling of “Hezbollah” (also known as “Hizbullah” and “Hizbu’llah”), is based on region and dialect, but all translate to the “Party of Allah.” As used herein, Hezbollah and Hizbullah refer to a Shiite Muslim political party and militant group the United States and European Union consider a foreign terrorist organization.

<sup>9</sup> The Coalition Forces were comprised of armed service members from the United States, United Kingdom, Australia, Spain, and Poland.

16. At one point, Iranian-backed violence accounted for half the attacks on Coalition Forces in Iraq.

17. Iran's terrorism campaign in Iraq was directly overseen by the IRGC-QF, Hezbollah, and cell leaders in Iraq.

18. The IRGC-QF was responsible for the creation of Hezbollah in 1983, and Hezbollah is one of the most influential groups the IRGC-QF has created.

19. Hezbollah serves as a proxy for Iran to support terrorists in Iraq.

20. As the *New York Times* recently noted in an article titled "Hezbollah: Iran's Middle East Agent, Emissary and Hammer,"

Hezbollah is involved in nearly every fight that matters to Iran and, more significantly, has helped recruit, train and arm an array of new militant groups that are also advancing Iran's agenda.... Hezbollah has evolved into a virtual arm of Iran's Islamic Revolutionary Guards Corps, providing the connective tissue for the growing network of powerful militia... The roots of that network go back to the American invasion of Iraq in 2003, when Iran called on Hezbollah to help organize Iraqi Shiite militias that in the coming years killed hundreds of American troops and many more Iraqis.

21. Iran openly acknowledged its terroristic goals in Iraq. In 2003, for example, Ayatollah Ahmad Janati, the secretary general of Iran's Council of Guardians, called on Iraqis to commit attacks against U.S.-led forces in Iraq. Two months later, Coalition Forces uncovered a fatwa (religious edict) issued by Iran urging "holy fighters" in Iraq to attack U.S. nationals.

22. There is no question that Iran, during the Relevant Period, substantially and materially supported and promoted terrorism against U.S. nationals, including Plaintiffs, in Iraq.

23. The support included money, weapons, training, and advisors and solidified an operational relationship between Hezbollah and various "Special Groups." (The term "Special Groups" refers to terrorist organizations established and funded by Iran.)

24. For example, the IRGC-QF established and controlled a network of cells in Iraq the aim of which was to assassinate key leaders, support death squads, and distribute highly lethal weapons for use against American forces and Iraqi citizens.

25. The IRGC-QF developed a distribution channel for the transfer of weapons from Iran to Iraq through the Ilam region in western Iran, as well as other main supply routes.

26. The weapons included mortars, rockets, sniper rifles, road side bombs, bullets, and rocket propelled grenades (“RPGs”).

27. In December 2003, for instance, Iranian agents shipped 1,000 rocket-propelled grenades and several boxes of explosives from Iran to Iraqi terrorist groups.

28. Hezbollah and the IRGC-QF’s network of terrorist cells was responsible for firing Iranian rockets and mortars at Americans in Baghdad and at bases around Iraq.

29. One of the weapons supplied by the IRGC-QF is a device known as an explosively formed penetrator (“EFP”).

30. EFPs are highly lethal explosive devices capable of penetrating tank armor.

31. EFPs have been used in terrorist attacks in Iraq against U.S. forces since 2004 and were used in some of the attacks that injured or killed the Plaintiffs.

32. U.S. military forces estimated the IRGC-QF, alone, provided up to \$3 million worth of equipment and funding to terrorist groups in Iraq every month.

33. American officials estimated that Iran supplied at least \$100 - \$200 million per year to Iraqi terrorist groups, in addition to the \$70 million per year supplied to Badr Organization and the \$100 - \$200 million a year to Hezbollah.

34. Suffice it to say, Iran's large-scale campaign of terrorism in Iraq was an expensive undertaking, one that required access to billions of USDs, including Eurodollars,<sup>10</sup> because the USD is the currency of international terrorism and because Iran's own domestic currency, the Rial, is one of the world's least valued currencies and essentially worthless outside of Iran. And, of course, if Iran used its own currency to fund terrorism those funds could be traced back to Iran.

35. To obtain USDs, Iran needed access to the U.S. financial system. Defendants provided that access.

36. To Iran, Defendants were familiar faces. Many of Iran's state controlled banks had already developed relationships with these banks, long before the sanctions were implemented. Several Defendants even operated branches in Tehran.

37. During the Relevant Period, Defendants used the U.S. financial system in an illegal manner to funnel hundreds of billions of USDs to Iran and its Agents and Proxies.

38. This was illegal, and Defendants knew it.

39. In fact, since 1984, the U.S. government has implemented a host of laws designed to thwart Iran's sponsorship of terrorism.

40. These laws, with a few minor exceptions, prohibit financial trade and investment activities with Iran involving the U.S. financial system, including processing USD transactions.

41. Under these laws, banks in the United States are prohibited, among other things, from engaging in USD-clearing transactions for the benefit of Iran and Iranian entities.

---

<sup>10</sup> Eurodollar refers to a deposit denominated in USD maintained by a bank outside the United States. Payment transactions in the Eurodollar market are not typically settled by the physical transfer of USD-denominated banknotes from one counterparty to another. Instead, Eurodollar transactions are settled electronically in New York through a bank-owned clearinghouse and then maintained by book entries of credits and debits in the respective counterparties' accounting systems (based on the SWIFT-NET) messages sent between the counterparties and their correspondent banks.

42. These laws were fortified in the wake of the 9/11 attacks through the passage of the Patriot Act, which amended the Bank Secrecy Act and was intended to strengthen U.S. measures to prevent, detect, and prosecute international money laundering and the financing, directly and indirectly, of terrorism.

43. Defendants, knowing the type of USD transfers they wished to complete to and from Iranian entities was illegal, devised clever ways of evading the laws and the U.S. government's mechanisms of enforcement.

44. One such mechanism is related to international wire transfers and is administered and enforced by OFAC.

45. OFAC enforces economic sanctions by blocking sanctioned entities from accessing the U.S. banking system.

46. To block illegal financial transactions, OFAC mandates the use of filters that automatically flag transactions to or from sanctioned entities.

47. To evade the filtering mechanism, Defendants purposefully removed key information from the wire transfers, a practice known as “stripping.”

48. Defendants stripped the wire transfers of information that would trigger the detection systems; they would then manually re-enter the payment information so the transfer would be processed undetected by regulators. The transfers were executed through correspondent bank accounts in New York and through the Federal Reserve Bank in New York.

49. Defendants even provided expert advice to Iranian entities concerning how to deceive OFAC and ensure payments would be processed without delay or interference.

50. By intentionally disguising financial payments to and from USD-denominated accounts and conducting illicit trade-finance transactions on Iran's behalf, Defendants provided the billions of dollars of support Iran needed to fund its terrorism campaign in Iraq.

51. These resources enabled Iran to fund the Terrorist Groups and provide them the training and weapons necessary to perpetrate Iran's campaign of terror in Iraq.

52. Eventually, after many years, the scheme was uncovered by U.S. law enforcement, and Defendants entered into criminal plea agreements and deferred prosecution agreements.

53. Defendants admitted to willingly evading U.S. laws and regulations, conducting illicit trade-finance transactions, and intentionally disguising financial payments to and from USD-denominated accounts.

54. Defendants further admitted to laundering billions of dollars on behalf of Iran and Iran-sanctioned entities.

55. Defendants are liable under the ATA because each committed acts of international terrorism as defined in 18 U.S.C. § 2331. Those acts of international terrorism include, but are not limited to: (1) providing material support to terrorists designated under 18 U.S.C. § 2339A; (2) providing material support to designated foreign terrorist organizations under 18 U.S.C. § 2339B; (3) engaging in financial transactions with the government of a country designated under section 6j of the Export Administration Act; and (4) concealing the financing of terrorism under 18 U.S.C. § 2339C. Each of these acts were dangerous to human life and violate the criminal laws of the United States.

56. The amounts Defendants laundered were reflected in the various agreements they signed, as summarized in the following chart:

<b>Bank</b>	<b>Money laundered on behalf of sanctioned entities</b>
Deutsche Bank AG	\$10,860,000,000
HSBC Bank USA, N.A. and HSBC Holdings PLC	\$1,256,000,000
Commerzbank AG and Commerzbank AG, New York Branch	\$563,000,000
Barclays Bank PLC	\$298,000,000
BNP Paribas S.A.	\$160,000,000,000
Standard Chartered Bank	\$250,000,000,000
The Royal Bank of Scotland N.V.	\$523,000,000
Crédit Agricole S.A.; Crédit Agricole Corporate & Investment Bank	\$312,000,000
Credit Suisse AG	\$536,000,000

57. Defendants are liable under the ATA and JASTA for the injuries and deaths to Plaintiffs because they committed acts of international terrorism, as that term is defined in 18 U.S.C. § 2331.

58. Defendants are also liable under the ATA and JASTA because they provided material support and aided and abetted Iran and its Agents and Proxies, as well as the Terrorist Groups who committed acts of international terrorism, including the Terrorist Attacks detailed below.

59. Defendants are also liable under the ATA and JASTA for conspiring to commit acts of international terrorism by, among other things, channeling billions of USD in the form of currency, arms, equipment, and other material support to Hezbollah, the IRGC, and the Qods Force, which, in turn, trained, armed, supplied and funded Iran's terrorist agents in Iraq, thereby

providing them with the means to carry out their attacks against Plaintiffs and Plaintiffs' family members.

60. The object of the Conspiracy was to defeat the economic sanctions imposed by the U.S. government, which were put in place with the sole purpose of deterring, disrupting, and preventing acts of international terrorism, the very terrorist attacks at issue in this case.

61. The Terrorist Groups and Iran used these USDs and other substantial and material support, through its Agents and Proxies, to carry out the campaign of terror in Iraq that was designed to kill and maim U.S. nationals.

62. Defendants benefited from the Conspiracy by generating enormous fees. The more money they cleared, the more money they made; and the greater the scale of Iran's terrorism campaign, the greater the need for Defendants' involvement.

63. Each of the Terrorist Attacks were directly and proximately caused by the Defendant's knowing and intentional participation in the Conspiracy.

64. Without the massive, active, and intentional participation of Defendants in the Conspiracy with Iran and its Agents and Proxies, as well as the Terrorist Groups, Iran's goals of directing lethal terrorist attacks against U.S. nationals, including Plaintiffs, could not have occurred, and certainly would not have occurred on so large a scale, which involved thousands of terrorist attacks resulting in thousands of casualties and injuries, including the deaths and injuries to Plaintiffs or Plaintiffs' family members.

65. Plaintiffs were specifically targeted by the Terrorist Groups that perpetrated the Terrorist Attacks which were supported and advanced by the Conspiracy. As such, these Terrorist Attacks were expressly aimed at the United States and U.S. Nationals.

66. As detailed herein, Iran and its Agents and Proxies, with the necessary assistance of Defendants, trained, sheltered, funded, armed, equipped, and provided other material support to Iran and its Agents and Proxies which, in turn, trained, armed, supplied, sheltered, equipped, funded, and provided other material support to the Terrorist Groups, and infiltrated and co-opted Iraqi security forces in an effort to kill or maim U.S. nationals, including Plaintiffs, and to coerce the United States into withdrawing those forces and to terrorize Iraq's civilian population in order to increase Iran's own influence.

67. These Terrorist Attacks are precisely the type of conduct the ATA proscribes, and the type of conduct engaged in by Defendants—materially assisting Iran and its Agents and Proxies to evade world-wide sanctions in order to fund deadly terrorist attacks against U.S. nationals abroad—that gives rise to liability under the ATA and JASTA.

## **II. JURISDICTION AND VENUE**

### **A. THIS COURT HAS JURISDICTION OVER ALL CLAIMS AND ALL PARTIES.**

#### **1. Subject Matter Jurisdiction**

68. This Court has subject-matter jurisdiction over this case pursuant to 28 U.S.C. § 1331 and 18 U.S.C. § 2338 since all claims are being brought under 18 U.S.C. § 2333.

#### **2. Personal Jurisdiction**

69. This Court properly exercises personal jurisdiction over all of Defendants.

70. Personal jurisdiction is appropriate under Fed. R. Civ. P. 4(k)(1)(A) because each defendant is subject to personal jurisdiction in a court of general jurisdiction in New York state and personal jurisdiction comports with the U.S. Constitution.

71. Each defendant is subject to personal jurisdiction in a court of general jurisdiction in New York state pursuant to N.Y. C.P.L.R. 302 because this case arises out of Defendants' laundering of USD in New York by executing tens of thousands of fund transfers totaling

hundreds of billions of dollars through the Federal Reserve Bank of New York as well as Defendants' New York branches and correspondent accounts in New York.

72. Such activity constitutes "transacting business" within New York state pursuant to C.P.L.R. 302(a)(1).

73. Defendants sent or cleared USD payments through the U.S., including clearing done through U.S. subsidiaries.

74. Defendants maintained correspondent bank accounts at financial institutions in New York and utilized the accounts to effectuate a significant number of fund transfers on behalf of Iran and its Agents and Proxies.

75. Defendants purposefully directed their activities at residents of this forum, and this litigation results from injuries arising out of and related to those activities. Defendants' culpable conduct stems from their use of the Federal Reserve Bank of New York and the New York branches of other financial institutions.

76. Defendants fund-transfer activities also fall within C.P.L.R. 302(a)(2) because by executing the transfers Defendants committed tortious acts within New York state.

77. Pursuant to the Conspiracy, Defendants executed numerous USD transfers knowing (or being deliberately indifferent to the fact) the money would be used to provide material support and resources to a state sponsor of terror to enable terrorist organizations to carry out terrorist attacks, including the attacks in which the plaintiffs and their family members were injured or killed.

78. The transferred funds did in fact provide material support and resources to the terrorist groups who committed the acts of terrorism that caused injuries or death to plaintiffs and their family members.

79. Defendants deliberately and repeatedly directed their money laundering activities toward New York's banking system specifically and the United States generally by executing the nefarious fund transfers in New York and, in doing so, knowingly providing substantial financial support to terrorist groups whose aim was to target American interests generally by attacking United States nationals.

80. The financial support enhanced the Terrorist Groups' ability to plan, prepare for, and carry out the terrorist attacks.

81. Personal jurisdiction over Defendants comports with the Due Process Clause of the Fourteenth Amendment because Defendants purposefully availed themselves of the privilege of doing business in New York (by executing thousands of transfers worth billions of dollars) and because this lawsuit arises out of and relates to Defendants' deliberate and recurring contacts with and activity in New York state.

82. Congress issued findings when it enacted JASTA, indicating that personal jurisdiction is proper over entities that, like Defendants, "knowingly or recklessly contribute material support or resources, directly or indirectly, to persons or organizations that pose a significant risk of committing acts of terrorism that threaten the security of nationals of the United States or the national security, foreign policy, or economy of the United States, necessarily direct their conduct at the United States." Congress found that those entities "should reasonably anticipate being brought to court in the United States to answer for such activities."

83. Section 317 of the Patriot Act further shows that Defendants who are foreign entities should reasonably anticipate defending suit in the United States for their money-laundering activities directed towards this forum. It provides that district courts have jurisdiction over a defendant if service of process is made and "the foreign person commits an offense under

subsection (a) involving a financial transaction that occurs in whole or in part in the United States;” or “the foreign person is a financial institution that maintains a bank account at a financial institution in the United States.”

84. Defendants expressly aimed their illegal conduct at New York.

85. This Court’s exercise of personal jurisdiction over Defendants is proper, reasonable, and comports with traditional notions of fair play and substantial justice.

86. This Court therefore has specific personal jurisdiction over Defendants.

87. This Court also has specific personal jurisdiction over most of Defendants pursuant to the nationwide service of process provision of the Anti-Terrorism Act, 18 U.S.C. § 2334(a), which provides that “[a]ny civil action under section 2333 of this title against any person may be instituted in the district court of the United States for any district where any plaintiff resides or where any defendant resides or is served, or has an agent. Process in such a civil action may be served in any district where the defendant resides, is found, or has an agent.”

88. All Defendants can be served with process in the United States, with the exception of HSBC Holdings plc (“HSBC Holdings”), HSBC Middle East, and Bank Saderat.

89. This Court’s exercise of personal jurisdiction over said Defendants comports with the Due Process Clause of the Fifth Amendment to the U.S. Constitution.

90. Said Defendants have sufficient minimum contacts with the United States as a whole and they purposefully availed themselves of the benefit the U.S. banking system when they executed the numerous illegal fund transfers.

91. This Court also has general personal jurisdiction over the following Defendants, who, as detailed below, are either headquartered in New York or have their principal place of

business in New York: HSBC North America Holdings, Inc. (“HSBC North America”); HSBC Bank USA, N.A.; and Commerzbank AG, New York Branch.

**B. VENUE IS PROPER IN THIS COURT**

92. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to this lawsuit—to wit, the money laundering scheme involving thousands of illegal fund transfers totaling billions of dollars—occurred at New York bank branches, the Federal Reserve Bank in Manhattan, and other financial institutions located in New York.

93. Venue is also proper under 18 U.S.C. § 2334(a) because at least one defendant resides, was served, or has an agent in this District.

94. Venue is also proper in this district, in the alternative, pursuant to 28 U.S.C. § 1391(b)(3) because Defendants are subject to the Court’s personal jurisdiction with respect to this action.

**III. THE PLAINTIFFS & THE TERRORIST ATTACKS**

95. At issue in this case are fifty-five (55) separate attacks perpetrated by the Terrorist Groups who were materially supported by Iran and its Agents and Proxies that killed or injured Plaintiffs (the “Terrorist Attacks”).

96. During the Relevant Period, the injuries and deaths caused by Defendants to Plaintiffs were the result of acts of international terrorism as defined by 18 U.S.C. § 2331(1). Each act of international terrorism was committed, planned, or authorized by organizations designated as FTOs, SDGTs, SDTs, or SDNs, as of the date on which such acts of international terrorism were committed, planned, and/or authorized. Further, Defendants provided material support to, conspired with, aided, and abetted Iran in its commission of the Terrorist Attacks by, among other things, knowingly providing access to the U.S. financial system, U.S. currency,

funding and other material support to Iran and its Agents and Proxies, including the Terrorist Groups who committed the Terrorist Attacks.

97. All Plaintiffs physically injured or killed in Iraq were, at the time of their injury or extrajudicial killing, participating in a peacekeeping mission intended to contribute to the security of the United Nations Assistance Mission for Iraq, the Governing Council of Iraq and other institutions of the Iraqi interim administration, and key humanitarian and economic infrastructure.

98. Without Defendants' conduct and material support described herein, Iran and the Terrorist Groups would not have had the funding or material support necessary to carry out the Terrorist Attacks.

99. Sixty-four (64) plaintiffs are individuals who were injured in fifty-five different Terrorist Attacks that occurred in Iraq between December 17, 2003 and October 12, 2011 and who, as a result, experienced physical and mental pain and suffering and emotional distress. Three (3) plaintiffs are decedents, whose Estates bring claims for individuals who were killed in those attacks, as well as all heirs thereof. The remaining eighty-seven (87) plaintiffs are family members of the victims of those attacks and have experienced injuries including anxiety, severe mental anguish, extreme emotional distress, and loss of companionship as a result of their relatives' injuries or death.

100. The following Plaintiffs are United States' nationals injured or killed in the acts of international terrorism complained of herein, and estates and/or family members of such U.S. nationals.

**A. THE MARCH 2, 2008 ATTACK – BASRA**

**1. Plaintiff Timothy Joseph O’Sullivan**

101. Plaintiff Timothy Joseph O’Sullivan is a citizen of the United States and is domiciled in the State of Ohio.

102. On March 2, 2008, Timothy Joseph O’Sullivan, age 36, was serving as a peacekeeping serviceman in the U.S. Air Force and as Senior Advisor to British Forces stationed in Basra, Iraq.

103. Iranian-sponsored Terrorist Groups in Mr. O’Sullivan’s area of operation (“AO”) were awarding bounties for the killing, kidnapping, or maiming of Coalition service members. At the time, Mr. O’Sullivan held the rank of Captain, O-3. Higher bounties were placed on high-ranking officers, such as Mr. O’Sullivan.

104. At the time of the March 2, 2008 Terrorist Attack, Mr. O’Sullivan was performing his duties as the Senior Advisor to British forces while traveling in an armored Warrior Infantry Fighting Vehicle as part of a five-vehicle convoy.

105. Due to the high bounties being paid by and to Iranian-supported terrorists for American casualties, Mr. O’Sullivan was traveling in a British vehicle in order to reduce the chance of an attack.

106. The vehicle was hit and destroyed by a massive EFP explosion, severely injuring Mr. O’Sullivan.

107. Additionally, during Mr. O’Sullivan’s time in Basra, from approximately 2007 through 2008, his unit was attacked approximately 800 – 1,100 times with Iranian Improvised Rocket Assisted Munitions (“IRAMs”) rockets that were manufactured in or provided by Iran.

108. The weapons used to attack and injure Mr. O’Sullivan were an Iranian-manufactured EFP and Iranian-manufactured and supplied rockets, provided by Iran and/or its

Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

109. The Iranian-funded Special Group JAM has claimed responsibility for the EFP attack that resulted in injury to Mr. O'Sullivan.

110. JAM was trained and armed by Iran's IRGC-QF with the assistance of Hezbollah.

111. As a result of the March 2, 2008 attack and multiple rocket attacks, Timothy Joseph O'Sullivan has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**B. THE OCTOBER 12, 2011 ATTACK – COS GARY OWEN**

**1. Plaintiffs The Alldridge Family**

112. Plaintiff Brian Clark Alldridge is a citizen of the United States and is domiciled in the State of Texas.

113. On the night of October 12, 2011, Brian Clark Alldridge, age 35, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with rockets.

114. Mr. Alldridge was injured in the attack.

115. The weapons used to attack and injure Mr. Alldridge on October 12, 2011 were Iranian-manufactured/supplied rockets provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

116. As a result of the October 12, 2011 Terrorist Attack and the injuries he suffered, Brian Clark Alldridge has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

117. Plaintiff Joann Alldridge is a citizen of the United States and is domiciled in the State of Texas. She is the wife of Brian Clark Alldridge.

118. Plaintiff Andrew Charles Major is a citizen of the United States and is domiciled in the State of Texas. He is the son of Joann Alldridge and the stepson of Brian Clark Alldridge.

119. Plaintiff Ashley Meikel Major is a citizen of the United States and is domiciled in the State of Texas. She is the daughter of Joann Alldridge and the stepdaughter of Brian Clark Alldridge.

120. Plaintiff A.M.M., a minor, represented by her legal guardian Joann Alldridge, is a citizen of the United States and is domiciled in the State of Texas. She is the daughter of Joann Alldridge and the stepdaughter of Brian Clark Alldridge.

121. Plaintiff Ronald Alldridge is a citizen of the United States and is domiciled in the State of Washington. He is the father of Brian Clark Alldridge.

122. Plaintiff DiAnna Alldridge is a citizen of the United States and is domiciled in the State of Washington. She is the mother of Brian Clark Alldridge.

123. Plaintiff Todd Alldridge is a citizen of the United States and is domiciled in the State of Indiana. He is the brother of Brian Clark Alldridge.

124. As a result of the October 12, 2011 Terrorist Attack and the injuries suffered by Brian Clark Alldridge, Plaintiffs Joann Alldridge, Andrew Charles Major, Ashley Meikel Major, A.M.M., a Minor, Ronald Alldridge, DiAnna Alldridge, and Todd Alldridge, have incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**C. THE JULY 10, 2011 ATTACK – FORWARD OPERATING BASE GARRY OWEN**

**1. Plaintiffs The Niquette Family**

125. Plaintiff Sean M. Niquette is a citizen of the United States and is domiciled in the State of New York.

126. On July 10, 2011, Sean M. Niquette, age 25, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with rockets.

127. Mr. Niquette was injured in the attack.

128. The weapons used to attack and injure Mr. Niquette on July 10, 2011 were Iranian-manufactured/supplied rockets provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

129. The Iranian-supported Special Group known as Asa’ib Ahl Al Haq (“AAH”) was operating in the area around Forward Operating Base (“FOB”) Garry Owen at the time of the July 10, 2011 Terrorist Attack and have claimed responsibility for attacks against U.S. Forces at the time of the attack that injured Mr. Niquette.

130. As a result of the July 10, 2011 Terrorist Attack and the injuries he suffered, Sean M. Niquette has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

131. Plaintiff Lauren Niquette is a citizen of the United States and is domiciled in the State of New York. She is the spouse of Sean M. Niquette.

132. As a result of the July 10, 2011 Terrorist Attack and the injuries suffered by Sean M. Niquette, Plaintiff Lauren Niquette has past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**2. Plaintiff William M. Chinn**

133. Plaintiff William M. Chinn is a citizen of the United States and domiciled in the State of Texas.

134. On the morning of July 10, 2011, William M. Chinn, age 32, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with rockets.

135. Mr. Chinn was injured in the attack.

136. The weapons used to attack and injure Mr. Chinn on July 10, 2011 were Iranian-manufactured/supplied rockets provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

137. The Iranian-supported Special Group known as AAH was operating in the area around FOB Garry Owen at the time of the July 10, 2011 Terrorist Attack and have claimed responsibility for attacks against U.S. Forces at the time of the attack that injured Mr. Chinn.

138. As a result of the July 10, 2011 Terrorist Attack, and the injuries he suffered, William M. Chinn has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**D. THE JUNE 6, 2011 ATTACK – CAMP LOYALTY**

**1. Plaintiff Walter Leman Thomas**

139. Plaintiff Walter Leman Thomas is a citizen of the United States and is domiciled in the State of Florida.

140. Around 4:00 a.m. on June 6, 2011, Walter Leman Thomas, age 22, was serving as a peacekeeping serviceman in the U.S. Army when he was in a rocket attack.

141. Mr. Thomas was injured in the attack.

142. The weapon used to attack and injure Mr. Thomas was an Iranian-

manufactured/supplied IRAM rocket provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

143. The Special Group known as Kata'ib Hizballah was operating in the area around FOB Loyalty, and has claimed responsibility for attacks against U.S. Forces at the time of the attack that injured Mr. Thomas. Kata'ib Hizballah perpetrated the Terrorist Attack that resulted in Plaintiff Mr. Thomas's injuries.

144. As a result of the June 6, 2011 Terrorist Attack, and the injuries he suffered, Walter Thomas has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**E. THE FEBRUARY 16, 2011 ATTACK—ROUTE TOMATOES, BAGHDAD, NEAR SADR CITY**

**1. Plaintiff Walter Leman Thomas**

145. Plaintiff Walter Leman Thomas is a citizen of the United States and is domiciled in the State of Florida.<sup>11</sup>

146. On February 16, 2011, Walter Leman Thomas, age 22, was serving as a peacekeeping serviceman in the U.S. Army when the Humvee he was in was attacked with an IED.

147. Mr. Thomas was injured in the attack.

148. The weapon used to attack and injure Walter Thomas was an Iranian-manufactured/supplied IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

---

<sup>11</sup> Plaintiff Walter Leman Thomas was also injured in the above-mentioned June 6, 2011 attack.

149. As a result of the February 16, 2011 Terrorist Attack, and the injuries he suffered, Walter Thomas has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**F. THE NOVEMBER 20, 2009 ATTACK – SUPPLY ROUTE OF KALZOO**

**1. Plaintiffs The Holladay Family**

150. Plaintiff Joshua Lionel Holladay is a citizen of the United States and is domiciled in the State of Alabama.

151. In the early morning of November 20, 2009, Joshua Lionel Holladay, age 26, was serving as a peacekeeping serviceman in the U.S. Army National Guard when a convoy he was in was attacked with an EFP.

152. Mr. Holladay was injured in the attack.

153. The weapon used to attack and injure Mr. Holladay was an Iranian-manufactured EFP provided by Iran and/or one of its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

154. As a result of the November 20, 2009 Terrorist Attack and the injuries he suffered, Joshua Lionel Holladay has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

155. Plaintiff Shirley Atkinson is a citizen of the United States and is domiciled in the State of Alabama. She is the mother of Joshua Lionel Holladay.

156. Plaintiff Crystal Hastings is a citizen of the United States and is domiciled in the State of Alabama. She is the sister of Joshua Lionel Holladay.

157. As a result of the November 20, 2009 Terrorist Attack and the injuries suffered by Joshua Lionel Holladay, Plaintiffs Shirley Atkinson and Crystal Hastings have incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**G. THE AUGUST 21, 2009 ATTACK – ROUTE IRISH, BAGHDAD**

**1. Plaintiff Randall Lavis Klingensmith**

158. Plaintiff Randall Lavis Klingensmith is a citizen of the United States and is domiciled in the State of Georgia.

159. On the morning of August 21, 2009, Randall Lavis Klingensmith, age 38, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an EFP.

160. Mr. Klingensmith was injured in the attack.

161. The weapon used to attack and injure Mr. Klingensmith on August 21, 2009 was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

162. As a result of the August 21, 2009 Terrorist Attack and the injuries he suffered, Randall Lavis Klingensmith has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**H. THE NOVEMBER 22, 2008 ATTACK –EN ROUTE TO FOB KALSU**

**1. Plaintiffs The Owen Family**

163. Plaintiff Michael L. Owen is a citizen of the United States and is domiciled in the State of Arizona.

164. On the afternoon of November 22, 2008, Michael L. Owen, age 24, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with multiple EFPs.

165. Mr. Owen was injured in the attack.

166. The weapons used to attack and injure Mr. Owen on November 22, 2008 were Iranian-manufactured EFPs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

167. The Iranian-supported Terrorist Group known as Jaysch al Mahdi (“JAM,” aka the “Mahdi Army”) was operating in the area around FOB Kalsu at the time of the November 22, 2008 Terrorist Attack, and has claimed responsibility for attacks against U.S. Forces at the time of the attack that injured Mr. Owen.

168. As a result of the November 22, 2008 Terrorist Attack and the injuries he suffered, Michael L. Owen has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

169. Plaintiff Laurie Miller is a citizen of the United States and is domiciled in the State of Kansas. She is the mother of Michael L. Owen.

170. Plaintiff R.O., a minor, represented by her legal guardian Michael L. Owen, is a citizen of the United States and is domiciled in the State of Kansas. She is the daughter of Michael L. Owen.

171. As a result of the November 22, 2008 Terrorist Attack and the injuries suffered by Michael L. Owen, Plaintiff Laurie Miller and R.O., a minor, have past and future noneconomic

damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

## **2. Plaintiffs The Williams Family**

172. Plaintiff Sean Lee Williams is a citizen of the United States and is domiciled in the State of Missouri.

173. On November 22, 2008, Sean Lee Williams, age 36, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked.

174. Mr. Williams was injured in the attack.

175. The weapons used to attack and injure Mr. Williams during the November 22, 2008 Terrorist Attack were Iranian-manufactured EFPs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

176. The Iranian-supported Terrorist Groups known as KH and JAM were operating in the area around FOB Kalsu at the time of the November 22, 2008 Terrorist Attack, and have claimed responsibility for attacks against U.S. Forces at the time of the attack that injured Mr. Williams.

177. As a result of the November 22, 2008 Terrorist Attack and the injuries he suffered, Sean Lee Williams has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

178. Plaintiff Sue Ann Williams is a citizen of the United States and is domiciled in the State of Missouri. She is the wife of Sean Lee Williams.

179. As a result of November 22, 2008 Terrorist Attack and the injuries suffered by Sean Lee Williams, Plaintiff Sue Ann Williams has past and future noneconomic damages,

including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**I. THE AUGUST 8, 2008 ATTACK – BAGHDAD**

**1. Plaintiffs The Morin/Harelston Family**

180. Plaintiff Baltazar Morin, Jr. is a citizen of the United States and is domiciled in the State of Texas.

181. On August 8, 2008, Baltazar Morin, Jr., age 19, was serving in the U.S. Army when the convoy he was in was attacked with an EFP.

182. Mr. Morin was injured in the attack.

183. The weapon used to attack and injure Mr. Morin was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

184. The Iranian-supported Special Group known as KH has claimed responsibility for the attack that resulted in injury to Mr. Morin.

185. As a result of the Attack and the injuries he suffered, Baltazar Morin, Jr. has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

186. Plaintiff Miranda Arispe Harelston is a citizen of the United States and is domiciled in the State of Texas. She is the sister of Baltazar Morin, Jr.

187. As a result of the August 8, 2008 Terrorist Attack and the injuries suffered by Baltazar Morin, Jr., Plaintiff Miranda Arispe Harelston has incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering,

loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**J. THE APRIL 28, 2008 ATTACK – FOB LOYALTY**

**1. Plaintiffs The Coe Family**

188. Plaintiff Thomas Milton Coe II is a citizen of the United States and is domiciled in the State of Texas.

189. On the morning of April 28, 2008, Thomas Milton Coe II, age 26, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with rockets.

190. Mr. Coe was injured in the attack.

191. The weapons used to attack and injure Mr. Coe were Iranian-manufactured/supplied rockets provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

192. As a result of the April 28, 2008 Terrorist Attack and the injuries he suffered, Thomas Milton Coe II has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

193. Plaintiff Heather Nicole Coe is a citizen of the United States and is domiciled in the State of Texas. She is the wife of Thomas Milton Coe II.

194. Plaintiff V.T.C., a minor, represented by his legal guardians Thomas Milton Coe II and Heather Nicole Coe, is a citizen of the United States and is domiciled in the State of Texas. He is the son of Thomas Milton Coe II and Heather Nicole Coe.

195. As a result of the April 28, 2008 Terrorist Attack and the injuries suffered by Thomas Milton Coe II, Plaintiffs Heather Nicole Coe and V.T.C., a minor, have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering,

loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**K. THE APRIL 13, 2008 ATTACK – SADR CITY**

**1. Plaintiff Michael James Bell**

196. Plaintiff Michael James Bell is a citizen of the United States and is domiciled in the State of Nevada.

197. On the afternoon of April 12, 2008, Michael James Bell, age 24, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with rockets.

198. Mr. Bell was injured in the attack.

199. The weapons used to attack and injure Mr. Bell were 120mm Katyusha rockets provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

200. As a result of the April 13, 2008 Terrorist Attack, and the injuries he suffered, Michael Bell has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**L. THE APRIL 8, 2008 ATTACK – MSR TAMPA**

**1. Plaintiffs The Collins Family**

201. Plaintiff Quentin D. Collins is a citizen of the United States and is domiciled in the State of New Mexico.

202. On April 8, 2008, Mr. Collins, age 49, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with IEDs.

203. Mr. Collins was injured in the attack.

204. The weapons used to attack and injure Mr. Collins on April 8, 2008 were IEDs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

205. As a result of the April 8, 2008 Terrorist Attack and the injuries he suffered, Quentin D. Collins has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

206. Plaintiff Melida Collins is a citizen of the United States and is domiciled in the State of New Mexico. She is the wife of Quentin D. Collins.

207. Plaintiff Siera Nicole Collins is a citizen of the United States and is domiciled in the State of California. She is the daughter of Quentin D. Collins.

208. Plaintiff Shawn Christopher Alan Collins is a citizen of the United States and is domiciled in the State of New Mexico. He is the son of Quentin D. Collins.

209. Plaintiff Michael Anthony Collins is a citizen of the United States and is domiciled in the State of New Mexico. He is the son of Quentin D. Collins.

210. Plaintiff I.C.C., a minor, represented by his legal guardians Quentin D. Collins and Melida Collins, is a citizen of the United States and is domiciled in the State of New Mexico. He is the minor son of Quentin D. Collins and Melida Collins.

211. As a result of the April 8, 2008 Terrorist Attack and the injuries suffered by Quentin D. Collins, Plaintiffs Melida Collins, Siera Nicole Collins, Shawn Christopher Alan Collins, Michael Anthony Collins, and I.C.C., a minor, have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**M. THE APRIL 4, 2008 ATTACK – VICTORY BASE COMPLEX, BAGHDAD**

**1. Plaintiffs The Von Letkemann Family**

212. Plaintiff Grant Blaney Von Letkemann II is a citizen of the United States and is domiciled in the State of Colorado.

213. On April 4, 2008, Grant Blaney Von Letkemann II, age 35, was serving as a peacekeeping serviceman as part of the Personal Security Detail for U.S. General David Petraeus, when he was attacked with rockets.

214. Mr. Von Letkemann was injured in the attack.

215. Mr. Von Letkemann was attacked with a 107 mm rocket. The remains of the rocket bore markings and stamps indicating the rocket had been manufactured in Iran just months before being used in Iraq.

216. The April 4, 2008 Terrorist Attack was committed by individuals associated with the Special Group JAM, which was trained and armed by Iran's IRGC-QF with the assistance of Hezbollah.

217. The weapon used to attack and injure Mr. Von Letkemann during the April 4, 2008 Terrorist Attack was an Iranian-manufactured rocket provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

218. As a result of the April 4, 2008 Terrorist Attack and the injuries he suffered, Grant Blaney Von Letkemann II, has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

219. Plaintiff Kelly Lynn Von Letkemann is a citizen of the United States and is domiciled in the State of Colorado. She is the wife of Grant Blaney Von Letkemann II.

220. As a result of April 4, 2008 Terrorist Attack and the injuries suffered by Grant Blaney Von Letkemann II, Plaintiff Kelly Lynn Von Letkemann has past and future noneconomic damages, including severe mental anguish, extreme emotionally pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**N. THE MARCH 26, 2008 ATTACK – FOB PHOENIX**

**1. Plaintiffs The Hernandez Family**

221. Plaintiff Ernesto P. Hernandez III is a citizen of the United States and is domiciled in the State of Virginia.

222. On the morning of March 26, 2008, Ernesto P. Hernandez, age 39, was serving as a peacekeeping serviceman in the U.S. Air Force when he was attacked with rockets.

223. Mr. Hernandez was injured in the attack.

224. The weapon used to attack and injure Mr. Hernandez on March 26, 2008 was an Iranian-manufactured/supplied rocket, provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

225. As a result of the March 26, 2008 Terrorist Attack and the injuries he suffered, Ernesto P. Hernandez III has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

226. Plaintiff Laura Fay Hernandez is a citizen of the United States and is domiciled in the State of Virginia. She is the wife of Ernesto P. Hernandez III.

227. Plaintiff E.H., a minor, represented by his legal guardians Ernesto P. Hernandez III and Laura Fay Hernandez, is a citizen of the United States and is domiciled in the State of Virginia. He is the son of Ernesto P. Hernandez III and Laura Fay Hernandez.

228. Plaintiff N.H., a minor, represented by his legal guardians Ernesto P. Hernandez III and Laura Fay Hernandez, is a citizen of the United States and is domiciled in the State of Virginia. He is the son of Ernesto P. Hernandez III and Laura Fay Hernandez.

229. Plaintiff Ernesto I. Hernandez II is a citizen of the United States and is domiciled in the State of Texas. He is the father of Ernesto P. Hernandez III.

230. As a result of the March 26, 2008 Terrorist Attack and the injuries suffered by Ernesto P. Hernandez III, Plaintiffs Laura Fay Hernandez, E.H., a minor, N.H., a minor, and Ernesto I. Hernandez II have incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**O. THE NOVEMBER 2, 2007 ATTACK – ROUTE SENATORS HIGHWAY, BAGHDAD**

**1. Plaintiffs The Poole Family**

231. Plaintiff James Joseph Poole III is a citizen of the United States and is domiciled in the State of Texas.

232. In the evening of November 2, 2007, Mr. Poole, age 24, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked by EFPs.

233. Mr. Poole was injured in the attack.

234. The weapons used to attack and injure Mr. Poole on November 2, 2007 were Iranian-manufactured EFPs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

235. As a result of the November 2, 2007 Terrorist Attack and the injuries he suffered, James Joseph Poole III has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

236. Plaintiff, Allison Poole Roosien is a citizen of the United States and is domiciled in the State of Michigan. She is the sister of James Joseph Poole III.

237. As a result of the November 2, 2007 Terrorist Attack and the injuries suffered by James Joseph Poole III, Plaintiff Allison Poole Roosien has past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**P. THE OCTOBER 31, 2007 ATTACK – SADR CITY, BAGHDAD**

**1. Plaintiff Koma Kekoa Texeira**

238. Plaintiff Koma Kekoa Texeira is a citizen of the United States and is domiciled in the State of Hawaii.

239. On the morning of October 31, 2007, Koma Kekoa Texeira, age 30, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an EFP.

240. Mr. Texeira was injured in the attack.

241. The weapon used to attack and injure Mr. Texeira was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

242. As a result of the October 31, 2007 Terrorist Attack and the injuries he suffered, Koma Kekoa Texeira has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**Q. THE SEPTEMBER 29, 2007 ATTACK - BAGHDAD**

**1. Plaintiff Eric James Atkinson**

243. Plaintiff Eric James Atkinson is a citizen of the United States and is domiciled in the State of Colorado.

244. On the afternoon of September 29, 2007, Eric Atkinson, age 28, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with an IED.

245. Mr. Atkinson was injured in the attack.

246. The weapon used to attack and injure Mr. Atkinson was an Iranian-manufactured/provided IED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

247. As a result of the September 29, 2007 Terrorist Attack, and the injuries he suffered, Eric Atkinson has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**R. THE SEPTEMBER 19, 2007 ATTACK – KADHIMIYA**

**1. Plaintiff Brian Robert Schar**

248. Plaintiff Brian Robert Schar is a citizen of the United States and is domiciled in the State of Colorado.

249. On September 19, 2007, Brian Robert Schar, age 25, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an EFP.

250. Mr. Schar was injured in the attack.

251. The weapon used to attack and injure Mr. Schar on September 19, 2007 was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

252. As a result of the September 19, 2007 Terrorist Attack and the injuries he suffered, Brian Robert Schar has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**S. THE SEPTEMBER 4, 2007 ATTACK – SADAR CITY, BAGHDAD**

**1. Plaintiffs The Mixson Family**

253. Plaintiff Joseph Catlin Mixson is a citizen of the United States and is domiciled in the State of Florida.

254. On the morning of September 4, 2007, Joseph Catlin Mixson, age 21, was serving as a peacekeeping serviceman in the U.S. Army when his patrol was attacked with an EFP.

255. Mr. Mixson was injured in the attack.

256. The weapon used to attack and injure Mr. Mixson on September 4, 2007 was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

257. As a result of the September 4, 2007 Terrorist Attack and the injuries he suffered, Joseph Catlin Mixson has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

258. Plaintiff Virginia BreAnn Mixson is a citizen of the United States and is domiciled in the State of Florida. She is the spouse of Joseph Catlin Mixson.

259. Plaintiff Joseph Johnson Mixson is a citizen of the United States and is domiciled in the State of Florida. He is the father of Joseph Catlin Mixson.

260. Plaintiff Karon Mixson is a citizen of the United States and is domiciled in the State of Florida. She is the mother of Joseph Catlin Mixson.

261. Plaintiff Alicia Mixson is a citizen of the United States and is domiciled in the State of Florida. She is the sister of Joseph Catlin Mixson.

262. As a result of the September 4, 2007 Terrorist Attack and the injuries suffered by Joseph Catlin Mixson, Plaintiffs Virginia BreAnn Mixson, Joseph Johnson Mixson, Karon Mixson, and Alicia Mixson have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**T. THE AUGUST 22, 2007 ATTACK – BAGHDAD/SADR CITY BORDER**

**1. Plaintiff Jerrald J. Jensen**

263. Plaintiff Jerrald J. Jensen is a citizen of the United States and is domiciled in the State of Colorado.

264. On August 22, 2007, Jerrald J. Jensen, age 37, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with EFPs.

265. Mr. Jensen was injured in the attack.

266. The weapons used to attack and injure Mr. Jensen were Iranian-manufactured EFPs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

267. As a result of the August 22, 2007 Terrorist Attack and the injuries he suffered during that attack, Jerrald J. Jensen has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**U. THE JULY 17, 2007 ATTACK – SADR CITY**

**1. Plaintiffs The Pearcy Family**

268. Plaintiff Colin Laird Pearcy is a citizen of the United States and is domiciled in the State of Illinois.

269. In the early morning hours of July 17, 2007, Colin Laird Pearcy, age 24, was serving as a peacekeeping serviceman in the U.S. Army when his patrol was attacked with an EFP.

270. Mr. Pearcy was injured in the attack.

271. The weapon used to attack and injure Mr. Pearcy on July 17, 2007 was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

272. As a result of the July 17, 2007 Terrorist Attack and the injuries he suffered, Colin Laird Pearcy has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

273. Plaintiff Laird Pearcy is a citizen of the United States and is domiciled in the State of Illinois. He is the father of Colin Laird Pearcy.

274. Plaintiff Anne Pearcy is a citizen of the United States and is domiciled in the State of Illinois. She is the mother of Colin Laird Pearcy.

275. Plaintiff Jody Striker is a citizen of the United States and is domiciled in the State of Illinois. She is the sister of Colin Laird Pearcy.

276. Plaintiff Karyn McDonald is a citizen of the United States and is domiciled in the State of Illinois. She is the sister of Colin Laird Pearcy.

277. Plaintiff Andrew Pearcy is a citizen of the United States and is domiciled in the State of Wisconsin. He is the brother of Colin Laird Pearcy.

278. Plaintiff Patrick Pearcy is a citizen of the United States and is domiciled in the State of Ohio. He is the brother of Colin Laird Pearcy.

279. As a result of the July 17, 2007 Terrorist Attack and the injuries suffered by Colin Laird Pearcy, Plaintiffs Laird Pearcy, Anne Pearcy, Jody Striker, Karyn McDonald, Andrew Pearcy, and Patrick Pearcy have incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

## **V. THE JULY 11, 2007 ATTACK – FORWARD OPERATING BASE HAMMER**

### **1. Plaintiffs The Smith Family**

280. Plaintiff Kevin Randall Smith is a citizen of the United States and domiciled in the State of Missouri.

281. On the day of July 11, 2007, Kevin Randall Smith, age 31, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with rockets.

282. Mr. Smith was injured in the attack.

283. The weapon used to attack and injure Mr. Smith on July 11th, 2007 was an Iranian-manufactured rocket provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

284. As a result of the July 11th, 2007 Terrorist Attack, and the injuries he suffered, Plaintiff Kevin Randall Smith has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

285. Plaintiff Jackay Smith is a citizen of the United States and is domiciled in the State of Missouri. She is the wife of Plaintiff Kevin Randall Smith.

286. Plaintiff D.S., a minor, represented by his legal guardians Kevin Randall Smith and Jackay Smith is a citizen of the United States and is domiciled in the State of Missouri. He is the son of Plaintiff Kevin Randall Smith and Jackay Smith.

287. Plaintiff L.S., a minor, represented by his legal guardians Kevin Randall Smith and Jackay Smith is a citizen of the United States and is domiciled in the State of Missouri. He is the son of Plaintiff Kevin Randall Smith and Jackay Smith.

288. Plaintiff Kayla Michelle Gulley is a citizen of the United States and is domiciled in the State of Missouri. She is the step-daughter of Plaintiff Kevin Randall Smith.

289. As a result of the July 11th, 2007 Terrorist Attack, and the injuries suffered by Plaintiff Kevin Randall Smith, Plaintiffs Jackay Smith, D.S., a minor, L.S., a minor, and Kayla Michelle Gulley have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**W. THE JULY 10, 2007 ATTACK – OBSERVATION POINT CAVALIER, TAJI**

**1. Plaintiffs The Segers Family**

290. Plaintiff Daniel Wayne Segers is a citizen of the United States and is domiciled in the State of Alabama.

291. On the afternoon of July 10, 2007, Daniel Wayne Segers, age 20, was serving as a peacekeeping serviceman in the U.S. Army when a vehicle he was in was attacked by an Iranian two-stage RPG.

292. Mr. Segers was injured in the attack.

293. The weapon used to attack the occupants of the Humvee on January 20, 2006 was an Iranian-manufactured/supplied dual-stage RPG-7 provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

294. As a result of the July 10, 2007 Terrorist Attack and the injuries he suffered, Daniel Wayne Segers has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

295. Plaintiff Larry Segers is a citizen of the United States and is domiciled in the State of Alabama. He is the father of Daniel Wayne Segers.

296. Plaintiff Sharon Wynona Parker is a citizen of the United States and is domiciled in the State of Alabama. She is the mother of Daniel Wayne Segers.

297. Plaintiff David Larry Segers is a citizen of the United States and is domiciled in the State of Alabama. He is the brother of Daniel Wayne Segers.

298. As a result of the July 10, 2007 Terrorist Attack and the injuries suffered by Daniel Wayne Segers, Plaintiffs Larry Segers, Sharon Wynona Parker, and David Larry Segers, have incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

## **X. THE JUNE 17, 2007 ATTACK – BASRA**

### **1. Plaintiff Grant Ransom Blackwell**

299. Plaintiff Grant Ransom Blackwell is a citizen of the United States and is domiciled in the State of South Carolina.

300. On the late afternoon of June 17, 2007, Grant Ransom Blackwell, age 25, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an EFP.

301. Mr. Blackwell was injured in the attack.

302. The weapon used to attack and injure Mr. Blackwell was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

303. As a result of the June 17, 2007 Terrorist Attack and the injuries he suffered, Grant Ransom Blackwell has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

#### **Y. THE MAY 31, 2007 ATTACK - BAGHDAD**

##### **1. Plaintiff John Maine**

304. Plaintiff John Maine is a citizen of the United States and is domiciled in the State of Oregon.

305. On the afternoon of May 31, 2007, John Maine, age 20, was serving as a peacekeeping serviceman in the U.S. Army, when a convoy he was in was attacked with an EFP.

306. Mr. Maine was injured in the attack.

307. The weapon used to attack and injure Mr. Maine was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

308. As a result of the May 31, 2007 Terrorist Attack and the injuries he suffered, John Maine has past and future noneconomic damages, including severe physical and mental pain and

suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**Z. THE MAY 28, 2007 ATTACK – SADR CITY**

**1. Plaintiff Gregory Edward Hogancamp**

309. Plaintiff Gregory Edward Hogancamp is a citizen of the United States and is domiciled in the State of Florida.

310. On May 28, 2007, Gregory Edward Hogancamp, age 24, was serving as a peacekeeping serviceman in the U.S. Army, when the tank he was in was attacked with an EFP.

311. Mr. Hogancamp was injured in the attack.

312. The weapon used to attack and injure Mr. Hogancamp during the May 28, 2007 Terrorist Attack was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

313. As a result of the May 28, 2007 Terrorist Attack and the injuries he suffered, Gregory Edward Hogancamp has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**AA. THE MAY 17, 2007 ATTACK – BAGHDAD**

**1. Plaintiffs The Gautier/Houchins Family**

314. Plaintiff Aaron Daniel Gautier was a citizen of the United States and was domiciled in the State of Virginia at the time of his death.

315. On May 17, 2007, Aaron Daniel Gautier, age 19, was serving as a peacekeeping serviceman in the U.S. Army when the vehicle he was in was attacked with an IED.

316. Mr. Gautier was killed in the attack.

317. The weapon used to kill Mr. Gautier was an improvised explosive device (“IED”) provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

318. The Iranian-supported Special Group known as KH has claimed responsibility for the attack that resulted in the death of Mr. Gautier.

319. Plaintiff Tina Louise Houchins is a citizen of the United States and is domiciled in the State of Virginia. She is the mother of Aaron Daniel Gautier.

320. Plaintiff Tina Louise Houchins brings an action individually, and on behalf of the Estate of Daniel Gautier, and all heirs thereof, as its legal representative.

321. Plaintiff Daniel Houchins is a citizen of the United States and is domiciled in the State of North Carolina. He is the father of Aaron Daniel Gautier.

322. Plaintiff Patricia Alexandria Gautier is a citizen of the United States and is domiciled in the State of Virginia. She is the sister of Aaron Daniel Gautier.

323. Plaintiff Alexis Houchins is a citizen of the United States and is domiciled in the State of Virginia. She is the sister of Aaron Daniel Gautier.

324. As a result of the May 17, 2007 Terrorist Attack and the injuries and death suffered by Aaron Daniel Gautier, Plaintiffs Tina Louise Houchins, Daniel Houchins, Patricia Alexandria Gautier, and Alexis Houchins, have experienced, and continue to experience, severe mental anguish, extreme emotional pain and suffering, medical expenses, funeral expenses, loss of their family member’s society, services, companionship, comfort, protection, instruction, advice and counsel, loss of earnings, income, and net accumulation to the Estate of Aaron Daniel Gautier.

**BB. THE APRIL 27, 2007 ATTACK – FALLUJAH, IRAQ**

**1. Plaintiff Guillermo Castillo**

325. Plaintiff Guillermo Castillo is a citizen of the United States and domiciled in the State of Florida.

326. During the daytime hours of April 27, 2007, Guillermo Castillo, age 28, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with an IED.

327. Mr. Castillo was injured in the attack.

328. The weapon used to attack and injure Mr. Castillo on April 27, 2007 was an Iranian-manufactured/provided IED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

329. As a result of the April 27, 2007 Terrorist Attack, and the injuries he suffered, Guillermo Castillo has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**CC. THE FEBRUARY 25, 2007 ATTACK – CSC SCANIA**

**1. Plaintiff Joshua Bradley Wolfe**

330. Plaintiff Joshua Bradley Wolfe is a citizen of the United States and is domiciled in the State of Washington.

331. On the night of February 25, 2007, Joshua Bradley Wolfe, age 27, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an EFP.

332. Mr. Wolfe was injured in the attack.

333. The weapon used to attack the convoy on February 25, 2007, and resulting in injury to Mr. Wolfe, was an Iranian-manufactured EFP provided by Iran and/or its Agents and

Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

334. As a result of the February 25, 2007 Terrorist Attack and the injuries he suffered, Joshua Bradley Wolfe has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**DD. THE FEBRUARY 3, 2007 ATTACK – ROUTE DOVER, SOUTH OF CAMP TAJI**

**1. Plaintiffs The Bass Family**

335. Plaintiff Travis Ryan Bass is a citizen of the United States and is domiciled in the State of Indiana.

336. On the morning of February 3, 2007, Mr. Bass, age 24, was serving as a peacekeeping serviceman in the U.S. Army when convoy he was in was attacked with EFPs.

337. Mr. Bass was injured in the attack.

338. The weapons used to attack and injure Mr. Bass on February 3, 2007 were Iranian-manufactured EFPs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

339. The Special Group KH has claimed responsibility for the attack that resulted in injury to Mr. Bass.

340. As a result of the February 3, 2007 Terrorist Attack and the injuries he suffered, Travis Ryan Bass has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

341. Plaintiff Harold C. Bass is a citizen of the United States and is domiciled in the State of Indiana. He is the father of Travis Ryan Bass.

342. Plaintiff Mary Louise Milton is a citizen of the United States and is domiciled in the State of Indiana. She is the mother of Travis Ryan Bass.

343. Plaintiff Allen Milton is a citizen of the United States and is domiciled in the State of Indiana. He is the stepfather of Travis Ryan Bass.

344. Plaintiff Aaron Bass is a citizen of the United States and is domiciled in the State of Indiana. He is the brother of Travis Ryan Bass.

345. Plaintiff Adam Christopher Bass is a citizen of the United States and is domiciled in the State of Indiana. He is the brother of Travis Ryan Bass.

346. Plaintiff Lisa Lambert is a citizen of the United States and is domiciled in the State of Indiana. She is the sister of Travis Ryan Bass.

347. As a result of the February 3, 2007 Terrorist Attack and the injuries suffered by Travis Ryan Bass, Plaintiffs Harold Carl Bass, Mary Louis Milton, Allen Milton, Aaron Bass, Adam Christopher Bass, and Lisa Lambert, have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**EE. THE JANUARY 27, 2007 ATTACK – ROUTE MICHIGAN, BAGHDAD**

**1. Plaintiffs The Nichols Family**

348. Plaintiff James R. Nichols is a citizen of the United States and is domiciled in the State of Virginia.

349. On the evening of January 27, 2007, James R. Nichols, age 30, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with rockets and RPGs.

350. Mr. Nichols was injured in the attack.

351. The weapons used to attack and injure Mr. Nichols on January 27, 2007 were Iranian-manufactured/supplied/ IED and RPGs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

352. As a result of the January 27, 2007 Terrorist Attack and the injuries he suffered, James R. Nichols has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

353. Plaintiff Queen Nichols is a citizen of the United States and is domiciled in the State of Illinois. She is the mother of James R. Nichols.

354. Plaintiff James Nichols is a citizen of the United States and is domiciled in the State of Illinois. He is the father of James R. Nichols.

355. Plaintiff Thomas Nichols is a citizen of the United States and is domiciled in the State of Illinois. He is the brother of James R. Nichols.

356. Plaintiff Sharon Nichols is a citizen of the United States and is domiciled in the State of Illinois. She is the sister of James R. Nichols.

357. As a result of the January 27, 2007 Terrorist Attack and the injuries suffered by James R. Nichols, Plaintiff's mother and father, Queen Nichols and James Nichols, and his brother and sister, Thomas Nichols and Sharon Nichols, have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**FF. THE DECEMBER 19, 2006 ATTACK - RAMADI**

**1. Plaintiff William Robert Biggs**

358. Plaintiff William Robert Biggs is a citizen of the United States and is domiciled in the State of California.

359. On the morning of December 19, 2006, William Biggs, age 20, was serving as a peacekeeping serviceman in the U.S. Marine Corps when he was attacked with an IED.

360. Mr. Bigg was injured in the attack.

361. The weapon used to attack and injure Mr. Biggs was an Iranian-manufactured/provided IED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

362. As a result of the December 19, 2006 Terrorist Attack, and the injuries he suffered, William Biggs has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**GG. THE NOVEMBER 27, 2006 ATTACK – SHULA**

**1. Plaintiffs The Strong Family**

363. Plaintiff Travis MacCody Strong is a citizen of the United States and is domiciled in the State of Colorado.

364. On the night of November 27, 2006, Travis MacCody Strong, age 29, was serving as a peacekeeping serviceman in the U.S. Army when his unit was attacked with an EFP.

365. Mr. Strong was injured in the attack.

366. The weapon used to attack and injure Mr. Strong on November 27, 2006 was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

367. As a result of the November 27, 2006 Terrorist Attack and the injuries he suffered, Travis MacCody Strong has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

368. Plaintiff Tayler Heston is a citizen of the United States and is domiciled in the State of Arizona. She is the mother of Travis MacCody Strong.

369. Plaintiff Anthony Joseph Durkacs is a citizen of the United States and is domiciled in the State of Nevada. He is the brother of Travis MacCody Strong.

370. As a result of the November 27, 2006 Terrorist Attack and the injuries suffered by Travis MacCody Strong, Plaintiffs Tayler Heston and Anthony Joseph Durkacs have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**HH. THE FEBRUARY 14, 2006 ATTACK – BAGHDAD**

**1. Plaintiff Tara Kathleen Hutchinson**

371. Plaintiff Tara Kathleen Hutchinson is a citizen of the United States and is domiciled in the State of Texas.

372. On the morning of February 14, 2006, Tara Kathleen Hutchinson, age 29, was serving as a peacekeeping servicewoman in the U.S. Army when her unit was attacked with an EFP.

373. Ms. Hutchinson was injured in the attack.

374. The weapon used to attack and injure Ms. Hutchinson was an Iranian-manufactured EFP provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

375. As a result of the February 14, 2006 Terrorist Attack and the injuries she suffered, Tara Kathleen Hutchinson, has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**II. THE OCTOBER 26, 2005 ATTACK – DUNBAR PROVINCE**

**1. Plaintiff Martin Sicairos**

376. Plaintiff Martin Sicairos is a citizen of the United States and is domiciled in the State of California.

377. On the morning of October 26, 2005, Martin Sicairos, age 26, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with IEDs, mortars, and RPGs.

378. Mr. Sicairos was injured in the attack.

379. The weapons used to attack and injure Mr. Sicairos were Iranian-manufactured/provided IEDs, mortars, and RPGs supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

380. As a result of the October 26, 2005 Terrorist Attack, and the injuries he suffered, Martin Sicairos has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**JJ. THE OCTOBER 8, 2005 ATTACK – RAMADI, IRAQ**

**1. Plaintiff Kade Luther Hinkhouse**

381. Plaintiff Kade Luther Hinkhouse is a citizen of the United States and domiciled in the State of Colorado.

382. On the morning of October 8, 2005, Kade Luther Hinkhouse, age 19, was serving as a peacekeeping serviceman in the U.S. Marine Corps when a convoy he was in was attacked with an IED.

383. Mr. Hinkhouse was injured in the attack.

384. The weapon used to attack and injure Mr. Hinkhouse on October 8, 2005 was an

Iranian-manufactured/supplied IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

385. As a result of the October 8, 2005 Terrorist Attack, and the injuries he suffered, Kade Luther Hinkhouse, has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**KK. THE SEPTEMBER 2, 2005 ATTACK - MOSUL**

**1. Plaintiff Ioan Adrian Kelemen**

386. Plaintiff Ioan Adrian Kelemen is a citizen of the United States and is domiciled in the State of Arizona.

387. On the night of September 2, 2005, Ioan Adrian Kelemen, age 33, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with an IED.

388. Mr. Kelemen was injured in the attack.

389. The weapon used to attack and injure Mr. Kelemen was an Iranian-manufactured IED provided by Iran and/or its agents to Iranian-funded and Iranian-trained terror operatives in Iraq.

390. The Iranian-funded and trained Foreign Terrorist Organization AAI was operating in the area at the time of the September 2, 2005 Terrorist Attack that injured Mr. Kelemen, and claimed responsibility for the attack.

391. As a result of the September 2, 2005 Terrorist Attack and the injuries he suffered, Ioan Adrian Kelemen has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**LL. THE AUGUST 26, 2005 ATTACK – HIT, IRAQ**

**1. Plaintiffs The Beyers Family**

392. Plaintiff Mark Howard Beyers is a citizen of the United States and domiciled in the State of New York.

393. On the Evening of August 26, 2005, Mark Beyers, age 26, was serving as a peacekeeping serviceman in the United States Marine Corps when he was attacked with an IED.

394. Mr. Beyers was injured in the attack.

395. The weapon used to attack and injure Mr. Beyers on August 26, 2005 was an Iranian-manufactured/provided IED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

396. As a result of the August 26, 2005 Terrorist Attack, and the injuries he suffered, Mark Beyers has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

397. Plaintiff Denise Beyers is a citizen of the United States and is domiciled in the State of New York. She is the wife of Mark Beyers.

398. As a result of the August 26, 2005 Terrorist Attack, and the injuries suffered by Mark Beyers, Plaintiff Denise Beyers has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of consortium, and past and future economic damages, including loss of services.

**MM. THE AUGUST 13, 2005 ATTACK – SADR CITY, IRAQ**

**1. Plaintiff Brad Lee Schwarz**

399. Plaintiff Brad Lee Schwarz is a citizen of the United States and is domiciled in the State of Illinois.

400. On August 13, 2005, Brad Lee Schwarz, age 20, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an EFP.

401. Mr. Schwarz was injured in the attack.

402. The weapons used to attack and injure Mr. Schwarz in the August 13, 2005 Terrorist Attack were Iranian-manufactured EFPs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

403. As a result of the August 13, 2005 Terrorist Attack and the injuries he suffered, Brad Lee Schwarz has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**NN. THE JULY 5, 2005 ATTACK – HIT, IRAQ**

**1. Plaintiffs The Cooley Family**

404. Plaintiff Joshua Jonathan Cooley is a citizen of the United States and domiciled in the State of Florida.

405. On the afternoon of July 5, 2005, Joshua Cooley, age 28, was serving as a peacekeeping serviceman in the U.S. Marine Corps when he was attacked with a Vehicle-Borne Improvised Explosive Device (“VBIED”).

406. Mr. Cooley was injured in the attack.

407. The weapon used to attack and injure Mr. Cooley on July 5, 2005 was an Iranian-manufactured/provided VBIED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

408. As a result of the July 5, 2005 Terrorist Attack, and the injuries he suffered, Joshua Jonathan Cooley has past and future noneconomic damages, including severe physical

and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

409. Plaintiff Christine Cooley is a citizen of the United States and is domiciled in the State of Florida. She is the mother and full-time caretaker of Joshua Cooley.

410. As a result of the July Terrorist Attack, and the injuries suffered by Joshua Cooley, Plaintiff Christine Cooley has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of consortium, and past and future economic damages, including loss of services

**OO. THE APRIL 19, 2005 ATTACK – ROUTE MIDLAND**

**1. Plaintiff Antonio Martinez Frederick**

411. Plaintiff Antonio Martinez Frederick is a citizen of the United States and is domiciled in the State of Mississippi.

412. On the morning of April 19, 2005, Antonio Martinez Frederick, age 33, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with IEDs.

413. Mr. Frederick was injured in the attack.

414. The weapon used in the April 19, 2005 Terrorist Attack that resulted in injury to Mr. Frederick were IEDs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

415. As a result of the April 19, 2005 Terrorist Attack and the injuries he suffered, Antonio Martinez Frederick has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**PP. THE APRIL 18, 2005 ATTACK – KARBALA**

**1. Plaintiff Wyman Harrell Jones**

416. Plaintiff Wyman Harrell Jones is a citizen of the United States and is domiciled in the State of Florida.

417. On the morning of April 18, 2005, Wyman Harrell Jones, age 42, was serving as a peacekeeping serviceman in the U.S. Army when a convoy he was in was attacked with an IED.

418. Mr. Jones was injured in the attack.

419. The weapon used to attack and injure Mr. Jones was an IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

420. As a result of the April 18, 2005 Terrorist Attack and the injuries he suffered, Wyman Harrell Jones has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**QQ. THE MARCH 15, 2005 ATTACK - BAGHDAD**

**1. Plaintiff Douglas Hamilton Kinard Jr.**

421. Plaintiff Douglas Hamilton Kinard Jr. is a citizen of the United States and is domiciled in the State of Georgia.

422. On the morning of March 15, 2005, Douglas Kinard Jr., age 34, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with an IED.

423. Mr. Kinard was injured in the attack.

424. The weapon used to attack and injure Mr. Kinard was an Iranian-manufactured/provided IED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

425. As a result of the March 15, 2005 Terrorist Attack, and the injuries he suffered, Douglas Hamilton Kinard Jr. has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**RR. THE JANUARY 1, 2005 ATTACK – HADITHA**

**1. Plaintiffs The Kuniholm Family**

426. Plaintiff Jonathan F. Kuniholm is a citizen of the United States and is domiciled in the State of Oregon.

427. On the morning of January 1, 2005, Jonathan F. Kuniholm, age 33, was serving as a peacekeeping serviceman in the U.S. Marine Corps when his patrol was attacked with an IED.

428. Mr. Kuniholm was injured in the attack.

429. The weapon used to attack and injure Mr. Kuniholm during the January 1, 2005 Terrorist Attack was an IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

430. The Iranian-supported FTO known as Ansar al Islam (“AAI”) was operating in the area around Haditha, and has claimed responsibility for attacks against U.S. Forces at and near the time of the attack that injured Mr. Kuniholm.

431. The tactics, techniques, and procedures employed in the attack against Mr. Kuniholm were taught to AAI terrorists by the Iranian IRGC-QF and Hezbollah in training camps in Iran.

432. As a result of the January 1, 2005 Terrorist Attack and the injuries he suffered, Jonathan F. Kuniholm has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

433. Plaintiff Michele Terese Quinn is a citizen of the United States and is domiciled in the State of Oregon. She is the wife of Jonathan F. Kuniholm.

434. Plaintiff S.K., a minor, represented by his legal guardians Jonathan F. Kuniholm and Michele Terese Quinn is a citizen of the United States and is domiciled in the State of Oregon. He is the son of Jonathan F. Kuniholm and Michele Terese Quinn.

435. Plaintiff Bruce Kuniholm is a citizen of the United States and is domiciled in the State of North Carolina. He is the father of Jonathan F. Kuniholm.

436. Plaintiff Elizabeth Kuniholm is a citizen of the United States and is domiciled in the State of North Carolina. She is the mother of Jonathan F. Kuniholm.

437. Plaintiff Erin Kuniholm is a citizen of the United States and is domiciled in the State of Oregon. She is the sister of Jonathan F. Kuniholm.

438. As a result of the January 1, 2005 Terrorist Attack and the injuries suffered by Jonathan F. Kuniholm, Plaintiffs Michele Terese Quinn, S. K., a minor, Bruce Kuniholm, Elizabeth Kuniholm, and Erin Kuniholm have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**SS. THE DECEMBER 21, 2004 ATTACK – FOB MAREZ, MOSUL**

439. On December 21, 2004, a suicide bomber entered the mess hall and approached a large group of U.S. soldiers, detonating himself and killing twenty-two people. At the time, this was the single deadliest suicide attack on American soldiers in Iraq, with fourteen U.S. soldiers killed. Seventy-two other personnel were injured in the attack carried out by a suicide bomber wearing an explosive vest and the uniform of the Iraqi security services. All the victims were in or near the Dining Hall at the FOB located next to the main U.S. military airfield at Mosul.

440. The Iranian-supported FTO Ansar al-Islam immediately claimed responsibility for the attack. In its claim of responsibility, AAI said the suicide bomber was a 24-year-old man from Mosul who worked at the base for two months and had provided information about the base to the group.

441. Moreover, in subsequent sworn Detainee Statements, individuals with knowledge of the planning and preparation of the attack, as well as those considered responsible for its coordination, admitted they were members of the FTO AAI (a/k/a Ansar al Sunna).

442. Weeks before the attack, soldiers from the base intercepted a document that mentioned a proposal for a massive “Beirut”-type attack on U.S. forces. The reference was to the techniques, tactics, and procedures utilized in the 1983 Beirut barracks bombing funded by Iran and committed by Hezbollah and Iranian Ministry of Intelligence and Security (“MOIS”) agents.

443. The weapon used in the December 21, 2004 Terrorist Attack to injure or kill the victims was provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

444. The training, tactics, and procedures employed in the December 21, 2004 Terrorist Attack were taught to Iranian-funded and Iranian-trained terror operatives in Iraq.

### **1. Plaintiffs The Ruhren Family**

445. Plaintiff David Alan Ruhren was a citizen of the United States and was domiciled in the State of Virginia at the time of his death.

446. On the morning of December 21, 2004, David Alan Ruhren, age 20, was serving as a peacekeeping serviceman in the U.S. Army.

447. Mr. Ruhren was killed in the attack.

448. Plaintiff Sonja Ruhren is a citizen of the United States and is domiciled in the State of Virginia. She is the mother of David Alan Ruhren.

449. Plaintiff Sonja Ruhren, brings an action individually, and on behalf of the Estate of David Alan Ruhren, and all heirs thereof, as its legal representative.

450. As a result of the December 21, 2004 Terrorist Attack and the injuries suffered by, and death of, David Alan Ruhren, Plaintiff Sonja Ruhren has experienced, and continues to experience, severe mental anguish, extreme emotional pain and suffering, and loss of her son's society, companionship, comfort, advice, and counsel.

## **2. Plaintiff Mark Joseph Pratt**

451. Plaintiff Mark Joseph Pratt is a citizen of the United States and is domiciled in the State of Virginia.

452. On the morning of December 21, 2004, Mark Joseph Pratt, age 39, was serving as a peacekeeping serviceman in the U.S. Army National Guard.

453. Mr. Pratt was injured in the attack.

454. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Mark Joseph Pratt has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

## **3. Plaintiff Evan Wayne Byler**

455. Plaintiff Evan Wayne Byler is a citizen of the United States and is domiciled in the State of Idaho.

456. At the time of the December 21, 2004 Terrorist Attack, Evan Wayne Byler, age 27, was serving as a peacekeeping serviceman in the U.S. Army National Guard.

457. Mr. Byler was injured in the attack.

458. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Evan Wayne Byler has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**4. Plaintiff Teray Anton Bundy**

459. Plaintiff Teray Anton Bundy is a citizen of the United States and is domiciled in the State of Virginia.

460. On December 21, 2004, Mr. Bundy, age 22, was serving as a peacekeeping serviceman in the U.S. Army National Guard.

461. Mr. Bundy was injured in the attack.

462. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Teray Anton Bundy has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**5. Plaintiff Jeff McKinley Wright**

463. Plaintiff Jeff McKinley Wright is a citizen of the United States and is domiciled in the State of Virginia.

464. On December 21, 2004, Mr. Wright, age 20, was serving as a peacekeeping serviceman in the U.S. Army National Guard.

465. Mr. Wright was injured in the attack.

466. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Jeff McKinley Wright has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**6. Plaintiffs The Turay Family**

467. Plaintiff Brima Charles Turay is a citizen of the United States and is domiciled in the State of Virginia.

468. Mr. Turay, age 21, was serving as a peacekeeping serviceman in the U.S. Army National Guard.

469. Mr. Turay was injured in the attack.

470. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Brima Charles Turay has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

471. Plaintiff Ruth Turay is a citizen of the United States and is domiciled in the State of Maryland. She is the mother of Brima Charles Turay.

472. As a result of the December 21, 2004 Terrorist Attack and the injuries suffered by Brima Charles Turay, Plaintiff Ruth Turay has past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of consortium, and past and future economic damages, including loss of services.

**7. Plaintiff Daniel Bivens**

473. Plaintiff Daniel Bivens is a citizen of the United States and is domiciled in the State of Tennessee.

474. On December 21, 2004, Daniel Bivens, age 21, was serving as a peacekeeping serviceman in the U.S. Army.

475. Mr. Bivens was injured in the attack.

476. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Daniel Bivens has past and future noneconomic damages, including severe physical and mental

pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**8. Plaintiff Eric James Atkinson**

477. Plaintiff Eric James Atkinson is a citizen of the United States and is domiciled in the State of Colorado.<sup>12</sup>

478. On the afternoon of December 21, 2004, Eric Atkinson, age 25, was serving as a peacekeeping serviceman in the U.S. Army.

479. Mr. Atkinson was injured in the attack.

480. As a result of the December 21, 2004 Terrorist Attack, and the injuries he suffered, Eric Atkinson has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**9. Plaintiff Angela Konen**

481. Plaintiff Angela Konen is a citizen of the United States and is domiciled in the State of Washington.

482. On the afternoon of December 21, 2004, Angela Konen, age 28, was serving as a peacekeeping servicewoman in the U.S. Army.

483. Ms. Konen was injured in the attack.

484. As a result of the December 21, 2004 Terrorist Attack, and the injuries she suffered, Angela Konen has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

---

<sup>12</sup> Plaintiff Eric James Atkinson was also injured in the above-mentioned September 29, 2007 attack.

**10. Plaintiff Jonathan B. Hogge**

485. Plaintiff Jonathan B. Hogge is a citizen of the United States and is domiciled in the State of Washington.

486. Mr. Hogge, age 21, was serving as a peacekeeping serviceman in the U.S. Army.

487. Mr. Hogge was injured in the attack.

488. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Jonathan B. Hogge has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**11. Plaintiff James Michael Ohrt**

489. Plaintiff James Michael Ohrt is a citizen of the United States and is domiciled in the State of Washington.

490. Mr. Ohrt, age 26, was serving as a peacekeeping serviceman in the U.S. Army.

491. Mr. Ohrt was injured in the attack.

492. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, James Michael Ohrt has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**12. Plaintiffs The Williams Family**

493. Plaintiff George Lon Williams is a citizen of the United States and is domiciled in the State of Washington.

494. On the afternoon of December 21, 2004, George Lon Williams, age 36, was serving as a peacekeeping serviceman in the U.S. Army.

495. Mr. Williams was injured in the attack.

496. As a result of the December 21, 2004 Terrorist Attack, and the injuries he suffered, George Lon Williams has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

497. Plaintiff Elizabeth Grace Williams is a citizen of the United States and is domiciled in the State of Washington. She is the wife of George Lon Williams.

498. Plaintiff Kayleigh Ann Williams is a citizen of the United States and is domiciled in the State of Washington. She is the daughter of George Lon Williams.

499. Plaintiff Nickolas Alan Williams a citizen of the United States and is domiciled in the State of Washington. He is the son of George Lon Williams.

500. As a result of the December 21, 2004 Terrorist Attack, and the injuries suffered by George Lon Williams, Plaintiffs Elizabeth Williams, Kayleigh Williams, and Nickolas Williams have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

### **13. Plaintiffs The Ward Family**

501. Plaintiff Antonio Harold Ward is a citizen of the United States and domiciled in the State of Oregon.

502. On the morning of December 21, 2004, Antonio Harold Ward, age 23, was serving as a peacekeeping serviceman in the U.S. Army.

503. Mr. Ward was injured in the attack.

504. As a result of the December 21, 2004 Terrorist Attack, and the injuries he suffered, Antonio Harold Ward, has past and future noneconomic damages, including physical

and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

505. Plaintiff Dennis Ward is a citizen of the United States and is domiciled in the State of Arizona. He is the father of Antonio Harold Ward.

506. Plaintiff Dallas Ward is a citizen of the United States and is domiciled in the State of Arizona. She is the mother of Antonio Harold Ward.

507. As a result of the December 21, 2004 Terrorist Attack, and the injuries suffered by Antonio Harold Ward, Plaintiffs Dennis Ward and Dallas Ward have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

#### **14. The Anderson Family**

508. Plaintiff Christopher Bryant Anderson is a citizen of the United States and is domiciled in the State of Texas.

509. On December 21, 2004, Christopher Bryant Anderson, age 24, was serving as a peacekeeping serviceman in the United States Army.

510. Mr. Anderson was injured in the attack.

511. As a result of the December 21, 2004 Terrorist Attack, and the injuries he suffered, Christopher Bryant Anderson has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

512. Plaintiff Tahnee Anderson is a citizen of the United States and is domiciled in the State of Texas. She is the wife of Christopher Bryant Anderson.

513. Plaintiff T.A.1, a minor, represented by her legal guardians Christopher Bryant Anderson and Tahnee Anderson, is a citizen of the United States and is domiciled in the State of Texas. She is the daughter of Christopher Bryant Anderson.

514. Plaintiff T.A.2, a minor, represented by her legal guardians Christopher Bryant Anderson and Tahnee Anderson, is a citizen of the United States and is domiciled in the State of Texas. She is the daughter of Christopher Bryant Anderson.

515. Plaintiff K.A, a minor, represented by her legal guardians Christopher Bryant Anderson and Tahnee Anderson, is a citizen of the United States and is domiciled in the State of Texas. She is the daughter of Christopher Bryant Anderson.

516. As a result of the December 21, 2004 Terrorist Attack and the injuries suffered by Christopher Bryant Anderson, Plaintiffs Tahnee Anderson, T.A.1, T.A.2, and K.A. have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of consortium, and past and future economic damages, including loss of services.

## **15. Plaintiffs The Collins Family**

517. Plaintiff Quentin D. Collins is a citizen of the United States and is domiciled in the State of New Mexico.<sup>13</sup>

518. On December 21, 2004, Quentin D. Collins, age 46, was serving as a peacekeeping serviceman in the U.S. Air Force.

519. On December 21, 2004, Quentin D. Collins was waiting to enter the dining facility (DFAC) at FOB Marez, Mosul, Iraq when an Iranian-affiliated suicide bomber detonated an explosive device in the DFAC. After the explosion, he entered the DFAC to assist in rendering aid. Approximately 1 to 1 ½ hours later he was counseling the injured who had been

---

<sup>13</sup> Plaintiff Quentin D. Collins was also injured in the above-mentioned April 8, 2008 attack.

transported to the hospital at FOB Diamondback which was located next to FOB Marez. While talking with injured soldiers, Mr. Collins heard several mortar strikes inside FOB Diamondback coming closer to his location. A mortar hit approximately five meters behind him. The explosion knocked him unconscious and shrapnel struck his lower back below his body armor. Between the time of the suicide bomber attacking the DFAC and the mortar attack, there was a small arms attack on the gate of FOB Diamondback. It was the conclusion of the command that all three attacks had been coordinated.

520. Mr. Collins was injured in the attack.

521. The weapon(s) used to attack and injure Mr. Collins on December 21, 2004 were Iranian-manufactured/supplied mortars provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

522. As a result of the December 21, 2004 Terrorist Attack and the injuries he suffered, Mr. Collins has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

523. Plaintiff Melida Collins is a citizen of the United States and is domiciled in the State of New Mexico. She is the wife of Quentin D. Collins.

524. Plaintiff Siera Nicole Collins is a citizen of the United States and is domiciled in the State of California. She is the daughter of Quentin D. Collins.

525. Plaintiff Shawn Christopher Alan Collins is a citizen of the United States and is domiciled in the State of New Mexico. He is the son of Quentin D. Collins.

526. Plaintiff Michael Anthony Collins is a citizen of the United States and is domiciled in the State of New Mexico. He is the son of Quentin D. Collins.

527. Plaintiff I.C.C., a minor, represented by his legal guardians Quentin D. Collins and Melida Collins, is a citizen of the United States and is domiciled in the State of New Mexico. He is the minor son of Quentin D. Collins and Melida Collins.

528. As a result of the December 21, 2004 Terrorist Attack and the injuries suffered by Quentin D. Collins, Plaintiffs Melida Collins, Siera Nicole Collins, Shawn Christopher Alan Collins, Michael Anthony Collins, and I.C.C., a minor, have past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of consortium, and past and future economic damages, including loss of services.

**TT. THE NOVEMBER 24, 2004 ATTACK - BAGHDAD**

**1. Plaintiffs The Fondren Family**

529. Plaintiff Jay Myrle Fondren is a citizen of the United States and is domiciled in the State of Texas.

530. On November 24, 2004, Jay Myrle Fondren, age 24, was serving as a peacekeeping serviceman in the U.S. Army when his patrol was attacked with IEDs.

531. Mr. Fondren was injured in the attack.

532. The weapon used to attack and injure Mr. Fondren was an IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

533. As a result of the November 24, 2004 Terrorist Attack and the injuries he suffered, Jay Myrle Fondren has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

534. Plaintiff Anne Hollingsworth Fondren is a citizen of the United States and is domiciled in the State of Texas. She is the spouse of Jay Myrle Fondren.

535. Plaintiff M.J.F., a minor, represented by his legal guardians Jay Myrtle Fondren and Anne Hollingsworth Fondren, is a citizen of the United States and is domiciled in the State of Texas. He is the son of Jay Myrtle Fondren and Anne Hollingsworth Fondren.

536. As a result of the November 24, 2004 Terrorist Attack and the injuries suffered by Jay Myrtle Fondren, Plaintiffs Anne Hollingsworth Fondren and M.J.F., a minor, have suffered past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of consortium, and past and future economic damages, including loss of services.

**UU. THE NOVEMBER 9, 2004 ATTACK – ISKANDARIYA**

**1. Plaintiffs The Nolte Family**

537. Plaintiff Nicholas S. Nolte was a citizen of the United States and is domiciled in the State of Nebraska at the time of his death.

538. On the morning of November 9, 2004, Nicholas S. Nolte, age 25, was serving as a peacekeeping serviceman in the U.S. Marine Corps when the vehicle he was in was attacked with an IED.

539. On November 24, 2004, Mr. Nolte died as result of his wounds sustained in the attack.

540. The weapon used to attack and kill Mr. Nolte on November 9, 2004 was an IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

541. The Special Group known as KH was operating in the area around FOB Kalsu and has claimed responsibility for attacks against U.S. Forces at the time of the attack that killed Mr. Nolte.

542. Plaintiff Melina Rose Nolte is a citizen of the United States and is domiciled in the State of Colorado. She is the widow of Nicholas S. Nolte.

543. Plaintiff Melina Rose Nolte brings an action individually, and on behalf of the Estate of Nicholas S. Nolte, and all heirs thereof, as its legal representative.

544. Plaintiff A.N., a minor, represented by her legal guardian Melina Rose Nolte, is a citizen of the United States and is domiciled in the State of Colorado. She is the daughter of Melina Rose Nolte and Nicholas S. Nolte.

545. Plaintiff Anita Nolte is a citizen of the United States and is domiciled in the State of Nebraska. She is the mother of Nicholas S. Nolte.

546. Plaintiff Jessica Nolte is a citizen of the United States and is domiciled in the State of Nebraska. She is the sister of Nicholas S. Nolte.

547. As a result of the November 9, 2004 Terrorist Attack and the injuries suffered by, and the resulting death of, Nicholas S. Nolte, Plaintiffs Melina Nolte, A.N., a minor, Anita Nolte, and Jessica Nolte have experienced, and continue to experience, severe mental anguish, extreme emotional pain and suffering, medical expenses, funeral expenses, loss of Nicholas N. Nolte's society, services, companionship, comfort, protection, instruction, advice and counsel, loss of earnings, income, and net accumulation to the estate of Nicholas N. Nolte.

## **VV. THE OCTOBER 31, 2004 ATTACK – FOB MAREZ, MOSUL, IRAQ**

### **1. Plaintiff Jonathan B. Hogge**

548. Plaintiff Jonathan B. Hogge is a citizen of the United States and is domiciled in the State of Washington.<sup>14</sup>

---

<sup>14</sup> Plaintiff Jonathan B. Hogge was also injured in the above-mentioned December 21, 2004 attack.

549. On October 31, 2004, Jonathan B. Hogge, age 21, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with an Iranian mortar.

550. Mr. Hogge was injured in the attack.

551. The weapon used to attack and injure Mr. Hogge on October 31, 2004 was an Iranian-manufactured/provided mortar supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

552. As a result of the October 31, 2004 Terrorist Attack, and the injuries he suffered, Jonathan B. Hogge, has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**WW. THE AUGUST 16, 2004 ATTACK – SADR CITY, BAGHDAD**

**1. Plaintiff David Allen Simmons II**

553. Plaintiff David Allen Simmons II is a citizen of the United States and is domiciled in the State of Alabama.

554. On the evening of August 16, 2004, David Allen Simmons II, age 20, was serving as a peacekeeping serviceman in the U.S. Army, when his patrol was attacked with Iranian RPGs.

555. Mr. Simmons was injured in the attack.

556. The weapon used to attack and injure Mr. Simmons was an Iranian-manufactured/supplied RPG provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

557. The Iranian-supported Special Group JAM was operating in the area at the time of the August 16, 2004 Terrorist Attack, and committed the attack that injured Mr. Simmons.

558. As a result of the August 16, 2004 Terrorist Attack and the injuries he suffered, David Allen Simmons II has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**XX. THE JUNE 29, 2004 ATTACK – CAMP FALLUJAH**

**1. Plaintiffs The Mills Family**

559. Plaintiff Hardy Pierce Mills IV is a citizen of the United States and is domiciled in the State of Texas.

560. On the morning of June 29, 2004, Hardy Pierce Mills IV, age 19, was serving as a peacekeeping serviceman in the U.S. Marines when he was attacked with an Iranian mortar.

561. Mr. Mills was injured in the attack.

562. The weapon used to attack and injure Mr. Mills on June 29, 2004 was a mortar provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

563. As a result of the June 29, 2004 Terrorist Attack, and the injuries he suffered, Hardy Pierce Mills IV, has incurred past and future noneconomic damages, including severe physical and mental pain and suffering, and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

564. Plaintiff Cathy Jean Mills is a citizen of the United States and is domiciled in the State of Texas. She is the mother of Hardy Pierce Mills IV.

565. Plaintiff Jacob Mills is a citizen of the United States and is domiciled in the State of Texas. He is the brother of Hardy Pierce Mills IV.

566. Plaintiff Joshua Mills is a citizen of the United States and is domiciled in the State of Texas. He the brother of Hardy Pierce Mills IV.

567. As a result of the June 29, 2004 Terrorist Attack and the injuries suffered by Hardy Pierce Mills IV, Plaintiffs Cathy Jean Mills, Jacob Mills, and Joshua Mills have incurred past and future noneconomic damages, including severe mental anguish, extreme emotional pain and suffering, loss of solatium, loss of consortium, and past and future economic damages, including loss of services.

**YY. THE JUNE 21, 2004 ATTACK – COMBAT OUTPOST APACHE**

**1. Plaintiff Arthur B. Stokenbury**

568. Plaintiff Arthur B. Stokenbury is a citizen of the United States and is domiciled in the State of Arkansas.

569. On the morning of June 21, 2004, Arthur B. Stokenbury, age 28, was serving as a peacekeeping serviceman in the U.S. Army National Guard when he was attacked with Iranian mortars.

570. Mr. Stokenbury was injured in the attack.

571. The weapons used to attack and injure Mr. Stokenbury were mortars provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

572. As a result of the June 21, 2004 Terrorist Attack and the injuries he suffered, Arthur B. Stokenbury has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**ZZ. THE APRIL 9, 2004 ATTACK – MARKET AREA OF BAIJI**

**1. Plaintiff Domenick Jared Alagna**

573. Plaintiff Domenick Jared Alagna is a citizen of the United States and is domiciled in the State of Texas.

574. On the afternoon of April 9, 2004, Domenick Jared Alagna, age 20, was serving as a peacekeeping serviceman in the U.S. Army when his unit was attacked with Iranian RPGs.

575. Mr. Alagna was injured in the attack.

576. The weapon used to attack and injure Mr. Alagna was an Iranian-manufactured/supplied RPG provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

577. The Iranian-supported FTO known as AAI was operating in Biaji, and has claimed responsibility for attacks against U.S. Forces at and near the time of the attack that injured Mr. Alagna.

578. The tactics, techniques, and procedures employed in the attack against Mr. Alagna were taught to AAI terrorists by the Iranian IRGC-QF and Hezbollah in training camps in Iran.

579. As a result of the April 9, 2004 Terrorist Attack and the injuries he suffered, Domenick Jared Alagna has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

#### **AAA. THE MARCH 13, 2004 ATTACK – KARBALA**

##### **1. Plaintiff Robert James Pearson**

580. Plaintiff Robert James Pearson is a citizen of the United States and is domiciled in the State of North Carolina.

581. On the morning of March 13, 2004, Robert Pearson, age 35, was serving as a peacekeeping serviceman in the U.S. Army when he was attacked with an IED.

582. Mr. Pearson was injured in the attack.

583. The weapon used to attack and injure Mr. Pearson was an Iranian-manufactured/provided IED supplied by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

584. As a result of the March 13, 2004 Terrorist Attack, and the injuries he suffered, Robert James Pearson has past and future noneconomic damages, including severe physical and mental pain and suffering and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**BBB. THE DECEMBER 23, 2003 ATTACK – SADR CITY, BAGHDAD**

**1. Plaintiff Roger Lee Young**

585. Plaintiff Roger Lee Young is a citizen of the United States and is domiciled in the State of Kentucky.

586. On the morning of December 23, 2003, Roger Lee Young, age 33, was serving as a peacekeeping serviceman in the U.S. Army when the vehicle he was in was attacked with an IED.

587. Mr. Young was injured in the attack.

588. The weapon used to attack and injure Mr. Young was an IED provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

589. The Iranian-supported Special Group JAM was operating in Sadr City and has claimed responsibility for attacks against U.S. Forces at and near the time of the attack that injured Mr. Young.

590. As a result of the December 23, 2003 Terrorist Attack and the injuries he suffered, Roger Lee Young has past and future noneconomic damages, including severe physical and

mental pain and suffering, and loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

**CCC. THE DECEMBER 17, 2003 ATTACK – SADR CITY**

**1. Plaintiff Allen Ryan Vaught**

591. Plaintiff Allen Ryan Vaught is a citizen of the United States and is domiciled in the State of Texas.

592. On the morning of December 17, 2003, Allen Ryan Vaught, age 32, was serving as a peacekeeping serviceman in the U.S. Army Reserve when a convoy he was in was attacked with IEDs.

593. Mr. Vaught was injured in the attack.

594. The weapons used to attack and injure Mr. Vaught were IEDs provided by Iran and/or its Agents and Proxies to Iranian-funded and Iranian-trained terror operatives, including the Terrorist Groups, in Iraq.

595. Subsequent investigation into the attack revealed the convoy's location and mission had been shared by tribal leaders with JAM terrorists.

596. The Iranian-supported Special Group JAM was operating in Sadr City and has claimed responsibility for attacks against U.S. Forces at and near the time of the attack that injured Mr. Vaught.

597. As a result of the December 17, 2003 Terrorist Attack and the injuries he suffered, Allen Ryan Vaught has past and future noneconomic damages, including severe physical and mental pain and suffering, loss of enjoyment of life, and past and future economic damages, including medical expenses, lost income, and loss of earning capacity.

#### **IV. ALL OF THE TERRORIST ATTACKS WERE ACTS OF INTERNATIONAL TERRORISM**

##### **A. THE ACTS COMMITTED BY THE TERRORIST GROUPS AND DEFENDANTS REFERENCED IN THE COMPLAINT WERE ACTS OF INTERNATIONAL TERRORISM PURSUANT TO 18 U.S.C. § 2331 ET. SEQ.**

598. Each Terrorist Attack appears to have been, and in fact was, intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, and/or to affect the conduct of a government by mass destruction, assassination, or kidnapping.

599. Each Terrorist Attack transcended national borders and/or occurred primarily outside the territorial jurisdiction of the United States or transcended national boundaries in terms of the means by which they were accomplished.

600. The acts of the Terrorist Groups, infra,<sup>15</sup> that injured and/or killed Plaintiffs were acts of international terrorism as defined by 18 U.S.C. § 2331 and were also acts constituting terrorist activities within the meaning of 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), and/or engaging in terrorism within the meaning of 22 U.S.C. § 2656f. All of the acts described herein involved violent acts – murder, attempted murder, assault, battery, providing funding and financial services required to commit such acts, and conspiring with and providing billions of dollars to designated state sponsors of terrorism, FTOs, SDTs and SDGTs, and/or SDNs. All such acts either violated the laws of the United States or would violate the criminal laws of the United States if the acts had been committed within the jurisdiction of the United States.

---

<sup>15</sup> As detailed below, al Qaeda, al Qaeda in Iraq, AAI/AAS, KH, JAM, AAH, Promised Day Brigades (“PDB”), and Badr are all Terrorist entities, but “Terrorist Groups” or “Groups” shall hereinafter include those groups *as well as* other as-of-yet unnamed FTOs, SDNs, SDGTs, and SDTs.

601. The deaths and injuries Plaintiffs sustained were the foreseeable and actual result of criminal acts of international terrorism.

602. The deaths and injuries Plaintiffs sustained were not the result of, nor did they occur in the course of, a declared war or an armed conflict between two or more nations.

603. The deaths and injuries Plaintiffs sustained were not the result of, nor did they occur in the course of, armed conflict between military forces of any origin.

604. None of the Terrorist Groups were “nations” for purposes of 18 U.S.C. § 2331.

605. None of the Terrorist Groups were “military forces” for purposes of 18 U.S.C. § 2331.

606. None of the Terrorist Groups conducted themselves substantially in conformance with the laws of war.

607. Each of the Terrorist Groups intentionally, and with extreme cruelty and violence, systematically violated the laws of war.

608. A substantial (and not incidental) portion of the violent activities of each Terrorist Group were directed against civilians, diplomats, peacekeepers, medical personnel, and noncombatants; in carrying out their violent attacks, the Terrorist Groups made no distinction between military personnel and civilians.

**B. THE UNITED STATES WAS NOT ENGAGED IN A WAR OR ARMED CONFLICT WITH IRAN DURING THE RELEVANT PERIOD.**

609. The United States has not declared war against Iran.

610. At no time during the Relevant Period, nor due to actions of the United States and Coalition Forces in Iraq, did the United States declare war or enact an Authorization for the use of military force against Iran. Nor did the United States or Coalition Forces engage in an armed

conflict with the military forces of Iran. Nor did Iran's military forces or their agents engage in lawful acts of war against Coalition Forces or U.S. nationals, including Plaintiffs.

611. At no time relevant to this Action did the United States engage in an armed conflict with the military forces of Iran. Nor did Iran's military forces or their agents engage in lawful acts of war against Coalition Forces and U.S. nationals, including Plaintiffs.

612. The Authorization for Use of Military Force Against Iraq Resolution of 2002, enacted October 16, 2002, was a joint resolution passed by the U.S. Congress authorizing limited military force against Iraq.

613. The United States has not enacted an Authorization for the use of military force against Iran, nor did the United States engage in an armed conflict with Iran or during the Relevant Period.

614. From a legal perspective, there is no such thing as a "war against terrorism,"<sup>16</sup> the nomenclature is merely a rhetorical device as terrorism is a phenomenon.

**C. THE INVASION OF IRAQ WAS AUTHORIZED BY UNITED NATIONS RESOLUTIONS UNDER CHAPTER VII OF THE U.N. CHARTER.**

615. Neither the 2003 invasion of Iraq, nor the Multi National Forces in Iraq ("MNF-I") presence within Iraq, has been officially classified as a war.

616. The position of the United States and the United Kingdom is the invasion was authorized under U.N. Security Council Resolutions 678 and 687, which specifically authorized the use of all necessary means to compel Iraq to comply with its international obligations.

---

<sup>16</sup> International Committee of the Red Cross, *Report on the applicability of IHL to terrorism and counterterrorism* (Oct. 1, 2015), <https://www.icrc.org/en/document/applicability-ihl-terrorism-and-counterterrorism>.

617. On November 8, 2002, the United Nations Security Council unanimously adopted Resolution 1441, under Chapter VII of the U.N. Charter, offering Iraq a final opportunity to comply with its disarmament obligations as set forth in numerous prior U.N.S.C. Resolutions.

618. On March 28, 2003, the United Nations Security Council, under Chapter VII of the U.N. Charter, unanimously adopted Resolution 1472.<sup>17</sup> The United States and the United Kingdom voted in favor of this resolution. The U.N. recognized the occupation of Iraq and provided, with the consent of the U.S. and U.K., the following:

- a) “Reaffirming the respect for the right of the people of Iraq to determine their own political future and to control their own natural resources;”
- b) “Reaffirming the commitment of all Member States to the sovereignty and territorial integrity of Iraq;”
- c) “Requests all parties concerned to strictly abide by their obligations under international law, in particular the Geneva Conventions and the Hague Regulations, including those relating to the essential civilian needs of the people of Iraq, both inside and outside Iraq.”

619. The conflict with the State of Iraq, under the rule of Saddam Hussein, lasted 21 days, from March 23, 2003 until May 1, 2003.

620. The U.N. Security Council has made no Article 39 finding of illegality; no illegal state of war existed.

**D. PRIOR TO JUNE 20, 2004, ALL U.S. FORCES AND CIVILIANS WERE PRESENT IN IRAQ IN ACCORDANCE WITH INTERNATIONAL LAW WITH THE GOAL TO RESTORE FULL SOVEREIGNTY TO THE IRAQI PEOPLE.**

621. On May 22, 2003, the United Nations Security Council unanimously passed Resolution 1483,<sup>18</sup> under Chapter VII of the U.N. Charter, which, *inter alia*:

---

<sup>17</sup> United Nations Security Council, *Resolution 1472* (Mar. 28, 2003), [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=S/RES/1472\(2003\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1472(2003)).

<sup>18</sup> United Nations Security Council, *Resolution 1483* (May 22, 2003), [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=S/RES/1483\(2003\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1483(2003)).

- a) Notes “the letter of 8 May 2003 from the Permanent Representatives of the United States of America and the United Kingdom of Great Britain and Northern Ireland to the President of the Security Council (S/2003/538) and recognizes the specific authorities, responsibilities, and obligations under applicable international law of these states as occupying powers under unified command (the “Authority”);”
- b) “Calls upon the Authority, consistent with the Charter of the United Nations and other relevant international law, to promote the welfare of the Iraqi people through the effective administration of the territory, including in particular working towards the restoration of conditions of security and stability and the creation of conditions in which the Iraqi people can freely determine their own political future;”
- c) “Calls upon all concerned to comply fully with their obligations under international law including in particular the Geneva Conventions of 1949 and the Hague Regulations of 1907;”
- d) “Supports the formation, by the people of Iraq with the help of the Authority and working with the Special Representative, of an Iraqi interim administration as a transitional administration run by Iraqis, until an internationally recognized, representative government is established by the people of Iraq and assumes the responsibilities of the Authority;”
- e) “Decides that, with the exception of prohibitions related to the sale or supply to Iraq of arms and related materiel other than those arms and related materiel required by the Authority to serve the purposes of this and other related resolutions, all prohibitions related to trade with Iraq and the provision of financial or economic resources to Iraq established by resolution 661 (1990) and subsequent relevant resolutions, including resolution 778 (1992) of 2 October 1992, shall no longer apply.”

622. On October 16, 2003, the United Nations Security Council unanimously passed Resolution 1511,<sup>19</sup> under Chapter VII of the U.N. Charter, which, *inter alia*:

- a) “Determines that the provision of security and stability is essential to the successful completion of the political process...and to the ability of the United Nations to contribute effectively to that process and the implementation of resolution 1483 (2003), and authorizes a multinational force under unified command to take all necessary measures to contribute to the maintenance of security and stability in Iraq, including for the purpose of ensuring necessary

---

<sup>19</sup> United Nations Security Council, *Resolution 1511* (Oct. 16, 2003), [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=S/RES/1511\(2003\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1511(2003)).

conditions for the implementation of the timetable and programme as well as to contribute to the security of the United Nations Assistance Mission for Iraq,”

- b) “Urges Member States to contribute assistance under this United Nations mandate, including military forces, to the multinational force referred to in paragraph 13 above;”
- c) “Emphasizes the importance of establishing effective Iraqi police and security forces in maintaining law, order, and security and combating terrorism consistent with paragraph 4 of resolution 1483 (2003);”
- d) “Unequivocally condemns the terrorist bombings of the Embassy of Jordan on 7 August 2003, of the United Nations headquarters in Baghdad on 19 August 2003, and of the Imam Ali Mosque in Najaf on 29 August 2003, and of the Embassy of Turkey on 14 October 2003, the murder of a Spanish diplomat on 9 October 2003, and the assassination of Dr. Akila al-Hashimi, who died on 25 September 2003, and emphasizes that those responsible must be brought to justice;”
- e) “Calls upon Member States to prevent the transit of terrorists to Iraq, arms for terrorists, and financing that would support terrorists, and emphasizes the importance of strengthening the cooperation of the countries of the region, particularly neighbours of Iraq, in this regard.”

**E. U.S. FORCES WERE PRESENT IN IRAQ SUBSEQUENT TO JUNE 19, 2004, AT THE INVITATION OF THE GOVERNMENT OF IRAQ AND PURSUANT TO A MANDATE BY THE UNITED NATIONS.**

623. On June 8, 2004, the United Nations Security Council passed Resolution 1546,<sup>20</sup>

which recognized the new government of Iraq, and:

- a) reaffirmed “the independence, sovereignty, unity, and territorial integrity of Iraq,”
- b) recognized the occupation of Iraq will end on June 20, 2004 and “Iraq will reassert its full sovereignty;”
- c) recognized “the Iraqi request for the continued presence of the multinational force and setting out its tasks, including by preventing and deterring terrorism, so that, *inter alia*, the United Nations can fulfil its role in assisting the Iraqi people . . . .”
- d) emphasized “the importance of developing effective Iraqi police, border enforcement, and the Facilities Protection Service, under the control of the Interior Ministry of Iraq, and, in the case of the Facilities Protection Service, other

---

<sup>20</sup> United Nations Security Council, *Resolution 1546* (June 8, 2004), <http://unscr.com/en/resolutions/1546>.

Iraqi ministries, for the maintenance of law, order, and security, including combating terrorism, and request[ed] Member States and international organizations to assist the Government of Iraq in building the capability of these Iraqi institutions;” and

- e) “[c]ondemn[ed] all acts of terrorism in Iraq, reaffirm[ed] the obligations of Member States under resolutions 1373 (2001) of 28 September 2001, 1267 (1999) of 15 October 1999, 1333 (2000) of 19 December 2000, 1390 (2002) of 16 January 2002, 1455 (2003) of 17 January 2003, and 1526 (2004) of 30 January 2004, and other relevant international obligations with respect, *inter alia*, to terrorist activities in and from Iraq or against its citizens, and specifically reiterate[d] its call upon Member States to prevent the transit of terrorists to and from Iraq, arms for terrorists, and financing that would support terrorists, and re-emphasizes the importance of strengthening the cooperation of the countries of the region, particularly neighbors of Iraq, in this regard.”

624. U.S. military personnel, including Plaintiffs, were not an occupying force in Iraq, but rather were in Iraq at the request of the Iraqi government and pursuant to international law and United Nations Security Council mandates under Chapter VII of the U.N. Charter.

**F. THE TERRORIST GROUPS WERE NOT “MILITARY FORCES” UNDER 18 U.S.C. § 2331 ET. SEQ.**

625. At all times during the Relevant Period, the Terrorist Groups intentionally conducted themselves as criminal terrorists and not as “military forces.”

626. Acts in the violation of the laws of war are not similar enough to other conduct explicitly covered by 18 U.S.C. § 2331(4)(c).<sup>21</sup>

627. The general practice of the Terrorist Groups was to take actions that violated the laws of war to a substantial degree and are not covered as acts of a ‘military’ force under 18 U.S.C. § 2331(4)(c).<sup>22</sup>

---

<sup>21</sup> *Gil v. Arab Bank Plc.*, 893 F. Supp. 2d 474, 483, 513-14 (E.D.N.Y. 2012) (citing *Estate of Kleiman v. Palestinian Authority*, 424 F. Supp. 2d 153, 162-67 (D.D.C. 2006); *Biton v. Palestinian Interim Self-Gov’t Authority*, 412 F. Supp. 2d 1, 6-11 (D.D.C. 2005)).

<sup>22</sup> *Gil*, 893 F. Supp. 2d at 517.

628. Organized and disciplined groups and national forces are, at minimum, required to comply with Article 3 common to the Geneva Conventions and with rules of customary International Humanitarian Law (“IHL”) during non-international conflicts, Articles 6, 7, and 8 of The Rome Statute of the International Criminal Court (“ICC Statute”), and during peacetime with International Human Rights Law (“IHRL”).

629. Each Defendant knew, or was indifferent to, the fact each of the Terrorist Groups:

- a) did not comply with any Articles or rules of the Geneva Conventions, IHL, or IHRL;
- b) intentionally violated the Articles and rules of Geneva Conventions, IHL, IHRL, and the ICC Statute;
- c) considered, in word and deed, all international laws of war and international human rights laws to be inapplicable to themselves;
- d) committed thousands of grave violations of the Articles and rules of the Geneva Conventions, IHL, IHRL, and the ICC Statute which were intentional and substantial and not accidental, unintended or incidental; and
- e) committed or intentionally or knowingly provided funding or material support for widespread and systematic campaigns of mass murder, mayhem, extrajudicial killings, ethnic cleansing, kidnapping, torture, terrorism, and indiscriminate violence against civilians, diplomats, law enforcement officers, peacekeepers, elected officials and medical personnel.

630. Armed conflict is a situation in which certain acts of violence are considered lawful and others are unlawful, but acts of terrorism are always unlawful, always penalized as criminal, and cannot be exempt from prosecution.<sup>23</sup>

631. At all times during the Relevant Period, each Defendant knew and/or was deliberately indifferent to the fact Iran sponsored and provided financing and access to international financial networks to the Terrorist Groups and that one of the primary reasons and

---

<sup>23</sup> International Committee of the Red Cross, *supra* note 16.

purposes of the sanctions was to prevent Iran from providing USDs and access to international financial networks to international terrorists.

632. At no time did any Defendant, in providing funding, financial services, and other material support to Iran, SDNs, and the Terrorists Groups, restrict the use of their funding and material support to activities other than international terrorism.

633. At no time relevant to this Action did the terrorist operatives who killed and injured Plaintiffs carry fixed distinctive signs recognizable at a distance, carry arms openly, conduct their operations in accordance with the laws and customs of war, or enjoy any form of combatant immunity for their acts.

**G. THE ATTACKS PERPETRATED BY THE TERRORIST GROUPS WERE CRIMINAL ACTS OF INTERNATIONAL TERRORISM AND NOT LEGITIMATE ATTACKS BY MILITARY FORCES DURING AN ARMED CONFLICT.**

634. Murder, attempted murder, kidnapping, torture, assault, and battery are still crimes even when committed against active military personnel.

635. The Department of Defense Law of War Manual states, “In contemporary parlance, private acts of hostility are often punished as ‘terrorism.’ The unauthorized use of violence by private persons to achieve political ends has been viewed as contrary to the principles of democratic States. Moreover, States have obligations under international law to repress terrorism, especially when conducted on their territory against other States.”<sup>24</sup>

636. “Acts of terrorism during armed conflict are prohibited by the law of war.”<sup>25</sup>

637. The attacks described herein were private acts of hostility and unauthorized use of violence by private persons to achieve political ends.

---

<sup>24</sup> U.S. Dep’t of Defense, *Law of War Manual*, Section 4.18.5, p.162 (June 2015, updated May 2016), <http://archive.defense.gov/pubs/Law-of-War-Manual-June-2015.pdf>.

<sup>25</sup> *Id.* at Section 3.4.2.3, p.86.

638. The Terrorist Attacks were intended to influence the United States and the United Nations by coercion (by coercing the withdrawal of Coalition Forces from Iraq) and to intimidate and coerce the Iraqi population.

639. Without Defendants' provision of such material support, on the scale that such support was provided, Iran and its Agents and Proxies would not have been able to conduct the thousands of acts of international terrorism on the scale and with the lethality they perpetrated, including the Terrorist Attacks, which caused the deaths, maiming, or otherwise injuring of Plaintiffs and Plaintiffs' family members.

640. The Terrorist Groups violated the following laws which, if perpetrated by a nation or by military forces, would be triable by a military commission under 10 U.S.C. § 950v:

- a) Attacking civilians (b)(2);
- b) Attacking civilian property (b)(3);
- c) Attacking protected property (b)(4);
- d) Taking hostages (b)(7);
- e) Using protected persons as a shield (b)(9);
- f) Using protected property as a shield (b)10);
- g) Torture (b)(11);
- h) Cruel or inhuman treatment (b)(12);
- i) Intentionally causing serious bodily injury (b)(13);
- j) Mutilating or maiming (b)(14);
- k) Murder in violation of the law of war (b)(14);
- l) Destruction of property in violation of the law of war (b)16);
- m) Using treachery or perfidy (b)(17);

- n) Improperly using a distinctive emblem (b)(19);
- o) Intentionally mistreating a dead body (b)(20);
- p) Rape (b)(21);
- q) Terrorism (b)(24);
- r) Providing material support for terrorism (b)(25);
- s) Wrongfully aiding the enemy (b)26; and
- t) Spying (b)(27).

641. Defendants violated the following laws which, if perpetrated by a nation or by military forces, would be triable by a military commission under 10 U.S.C. § 950v:

- a) Providing material support for terrorism<sup>26</sup> (b)(25);
- b) Wrongfully aiding the enemy<sup>27</sup> (b)(26); and
- c) Conspiracy (b)(28).

642. The conduct of Iran and/or the Terrorist Groups, violated the laws of war (including, e.g., AAH operatives masquerading as members of U.S. armed forces, targeting civilians and torturing and executing defenseless hostages; AAI operatives disguising themselves as Iraqi military and police in order to infiltrate FOBs and detonating suicide bombs, etc.), and the widespread and intentional attacks upon U.S. nationals (including Plaintiffs), British, Iraqi,

---

<sup>26</sup> 10 U.S.C. § 950v(b)(25), [https://www.gpo.gov/fdsys/pkg/USCODE-2008-title10-pdf/USCODE-2008-title10-subtitleA-partII-chap47A-subchapVII-sec950v.pdf](https://www.gpo.gov/fdsys/pkg/USCODE-2008-title10/pdf/USCODE-2008-title10-subtitleA-partII-chap47A-subchapVII-sec950v.pdf) (last visited Oct. 14, 2017).

(A) Offense.—Any person subject to this chapter who provides material support or resources, knowing or intending that they are to be used in preparation for, or in carrying out, an act of terrorism (as set forth in paragraph (24)), or who intentionally provides material support or resources to an international terrorist organization engaged in hostilities against the United States, knowing that such organization has engaged or engages in terrorism (as so set forth), shall be punished as a military commission under this chapter may direct.

(B) Material support or resources defined.—In this paragraph, the term “material support or resources” has the meaning given that term in section 2339A(b) of title 18.

<sup>27</sup> 10 U.S.C. § 950v(b)(26), *Wrongfully aiding the enemy*. “Any person subject to this chapter who, in breach of an allegiance or duty to the United States, knowingly and intentionally aids an enemy of the United States, or one of the co-belligerents of the enemy, shall be punished as a military commission under this chapter may direct.”

and other civilians and United Nations personnel, constituted a substantial, rather than an incidental, part of their objectives and conduct.

643. The Terrorist Groups failed to comply with, and intentionally violated, the laws of Distinction, Proportionality, Military Necessity, Unnecessary Suffering, Prohibition of Perfidy, Emblems of Nationality, Good Faith, and Humane Treatment and Non-Discrimination.

644. At all relevant times, each Defendant knew, or were deliberately indifferent to, the fact Iranian Agents and Proxies, as well as the Terrorist Groups, intentionally violated the Geneva Conventions, IHL, IHRL, and the ICC Statute, including specifically the laws of Distinction, Proportionality, Military Necessity, Unnecessary Suffering, Prohibition of Perfidy, Emblems of Nationality, Good Faith, and Humane Treatment and Non-Discrimination, Torture, Crimes against Humanity, and Genocide (ethnic cleansing).

645. Defendants knew, or were indifferent to, the fact the Terrorist Groups supported by Iran intentionally failed to distinguish between combatants and civilians or the civilian population; attacked civilians and/or the civilian population; failed to distinguish themselves from the civilian population while conducting terrorist attacks, did not wear identifiable uniforms or insignias, nor visually distinguish themselves from the Iraqi civilian populations; violated the laws of proportionality by using excessive force irrespective to the harm and mass murder of innocent civilians, including women and children; committed horrific acts of collective punishment and intimidation of civilian populations, and issued threats of mass and extreme violence, the primary purpose of which was to spread terror among the civilian population; and chose methods, weapons, and tactics intending to cause, and actually causing, unnecessary suffering or superfluous injury.

646. Defendants knew, or were indifferent to, the fact the Terrorist Groups intentionally treated civilians inhumanely and discriminated against people based on sex, nationality, race, religion, or political beliefs; perpetrated violent and illegal lethal attacks against hospitals, patients, medical personnel, and medical transport, and used the medical facilities to launch attacks, and house weapons and soldiers; deliberately committed widespread and systematic attacks directed against identifiable parts of the civilian populations, including acts of mass murder, extermination, enslavement, deportation or forcible transfer of populations, unlawful imprisonment, sexual violence, and other inhumane acts of a similar character intentionally causing great suffering.

647. Defendants knew, or were indifferent to, the fact the Terrorist Groups each deliberately attempt to destroy people on a large scale, committed purposeful actions to destroy a collectivity through mass or selective murders of group members, which also constituted ethnic cleansing.

648. Defendants knew, or were indifferent to, the fact the United Nations Security Council adopted Resolution 1618 on August 4, 2005,<sup>28</sup> which, *inter alia*:

- a) “Condemns without reservation and in the strongest terms the terrorist attacks that have taken place in Iraq, and regards any act of terrorism as a threat to peace and security;”
- b) “Takes note particularly of the shameless and horrific attacks in recent weeks which have resulted in over one hundred deaths, including thirty-two children, employees of the Independent Electoral Commission of Iraq, and a member and expert advisor of the commission charged with the drafting of a permanent constitution for a new, democratic Iraq....”

---

<sup>28</sup> United Nations Security Council, *Resolution 1618* (Aug. 4, 2005), [http://www.un.org/en/ga/search/view\\_doc.asp?symbol=S/RES/1618\(2005\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1618(2005)).

- c) "Further notes with great concern that attacks on foreign diplomats in Iraq have increased in number, and have resulted in the murder or kidnapping of such diplomats;"
- d) "Reaffirms the obligations of Member States under resolutions 1373...with respect, *inter alia*, to terrorist activities in and from Iraq or against its citizens, and specifically strongly urges Member States to prevent the transit of terrorists to and from Iraq, arms for terrorists, and financing that would support terrorists...;" and
- e) "Urges all States, in accordance with their obligations under resolution 1371 (2001), to cooperate actively in efforts to find and bring to justice their perpetrators, organizers and sponsors of these barbaric act."

#### **H. HEZBOLLAH**

649. Hezbollah is an international terrorist organization and not a "military force" and intentionally violates all core provisions of international humanitarian laws (laws of war), IHRL and the ICC Statutes.

650. Hezbollah has a long history of intentionally targeting civilians, diplomats, hospitals, religious institutions, and non-combatants, perpetrating acts of mass murder, assassinations and kidnappings intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions.

651. The United States has designated Hezbollah as an FTO, SDT, and SDGT.

652. The United Kingdom proscribed Hezbollah's External Security Organization as a terrorist organization in March 2001, and in 2008, the proscription was extended to its Military apparatus and Jihad Council.

653. The following countries and international organizations have also designated Hezbollah (or at least its violent "wing") as a terrorist organization: the Arab League; Australia;

Bahrain; Canada; European Union; France; Gulf Cooperation Council; Israel; Japan; Netherlands; New Zealand.<sup>29</sup>

654. Hezbollah recognizes and labels itself a terrorist organization with the goal of achieving political objectives through the use of violence. On February 16, 1985, Sheik Ibrahim al-Amin published Hezbollah's Manifesto, which states in part - "Our Objectives...the sons of Hezbollah know who are the major enemies in the Middle East – the Phalanges, Israel, France, and the U.S. The sons of our umma are now in a state of growing confrontation with them, and will remain so until the realization of the following three objectives: (a) to expel the Americans, the French, and their allies indefinitely from Lebanon..."

655. Hezbollah proudly publicized its militancy and its desire to spread it throughout the world. In an interview, Sheikh Naim Qassem, Hezbollah's deputy secretary general, proudly acknowledged his organization's efforts to pass its rich militant experience to other Iranian-aligned forces.

656. On May 24, 2004, Hezbollah leader Hassan Nasrallah delivered a speech during the annual Ashura Day ceremony (a Shiite holy day) in Beirut. In his speech, Nasrallah declared a jihad against the Coalition Forces in Iraq, including U.S. nationals. The speech specifically called for the all out jihad against Americans in Iraq, including Americans in the Shiite towns of Karbala and Najaf. Both of these towns are areas where JAM initiated massive battles against U.S. nationals from April 2004 until at least August 2004.

---

<sup>29</sup> Only China, Cuba, Iran, Iraq, North Korea, Russia, Syria, and Venezuela do not consider Hezbollah a terrorist organization.

657. In his speech, Narsallah incited and pledged to support not only for the Shiite special groups (which he refers to as “Resistance Groups,” but also for Sunni religious groups—which necessarily include AAI and al Qaeda. In relevant part, Narsallah stated as follows:

Our march today is to defend every grain of dust in Iraq and all its cities from Najaf to Karbala to Falluja to Al-Qaim to Baghdad to Basra and to Rafah and the olive and Gaza neighborhoods and to every location where there is a conflict between the resistance and the occupiers. . . Today in Iraq, what we demand is that the nation defends all of Iraq and the people of Iraq as a whole, from the entire Iraqi population and from the resistance<sup>30</sup> in all its forms in Iraq. . . There is one camp called America and “Israel,” and we say to this camp: Death to America...And we say to the same killers in Rafah, Najaf, and Karbala, and Qaim: Death to “Israel” . . . We know how to continue this battle to end the defeat of the enemy and our victory, we bear the burden of blood and loss and sacrifices, and I affirm that our solidarity with our people in Palestine and Rafah and our people in Iraq is not incompatible with our national interests, because here we do not pretend, we do not challenge our partners at home, but we challenge the enemies of our homeland and the enemies of our nation who if they managed to eliminate part of this nation will continue to eliminate the rest of this nation.<sup>31</sup>

658. In addition to committing the terrorist attacks which are the subject of this lawsuit, Hezbollah intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions. For example:

- a) On June 19, 1982, Hezbollah kidnapped David S. Dodge, president of the American University in Beirut;
- b) On March 16, 1984, Hezbollah kidnapped CIA Beirut Station Chief William Buckley, tortured him for 15 months and then murdered him;
- c) In 1989, Hezbollah kidnapped U.S. Marine Colonel William Higgins and held him hostage and tortured him to death over the course of two years, and then dumped his body into a street;

---

<sup>30</sup> The term “resistance” is a Hezbollah code word meaning armed struggle, including terrorism.

<sup>31</sup> See <https://archive.alahednews.com.lb/alahed.org/archive/2004/2805/file/doc1.htm> (last visited, Oct. 15, 2017) (translation to English available).

- d) During the 1980s, Hezbollah kidnapped, tortured, and held hostage approximately 30 other Westerners, including Terry Anderson (American AP journalist), Terry Waite (Assistant for Anglican Communion Affairs for the Archbishop of Canterbury), John McCarthy (British UPI journalist), and Father Lawrence Jenko;
- e) The April 18, 1983 suicide truck bombing of the U.S. embassy in Beirut, Lebanon, killing 63 and injuring other diplomats and civilians;
- f) The September 20, 1984 suicide truck bombing of the United States embassy annex building killed 23 and injured other civilians and diplomats;
- g) The June 14, 1985 hijacking of TWA Flight 847;
- h) The bombing of the Israeli embassy in London on July 26, 1994, by two Hezbollah terrorists, Jawad Botmen and Samar Alami, that killed 29 civilians, including 4 Israeli diplomats;
- i) On July 18, 1994, Ibrahim Hussein Berro, a Hezbollah operative, perpetrated a vehicle suicide bombing attack on the Asociacion Mutual Israelita Argentina building in Buenos Aires, Argentina, killing 85 and injuring hundreds of other civilians. In November 2007, Interpol entered the names of six individuals on its “red notice list,” for their role in the AMIA bombing. Included in the notice was Imad Mughniyah<sup>32</sup> (former head of Hezbollah terrorist operations and designated by the United States as an SDGT); Ali Fallahian, (Iranian Minister of Intelligence 1989-1997); Ahmad Reza Asghari (third secretary of the Iranian embassy in Buenos Aires “until his abrupt departure from Argentina” on July 1, 1994); Ahmad Vahidi (former commander of Qods Force); Mohsen Rezaee (former commander of the IRGC);
- j) The bombing of Alas Chiricanas Flight 901 that killed all 21 on board; and
- k) The bombing of a tourist bus in Burgas, Bulgarian on July 18, 2012 that killed 5 and injured 32 civilians (including Americans).

659. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services and material support to Hezbollah.

---

<sup>32</sup> Anthony Shadid & Alia Ibrahim, *Bombing Kills Top Figure in Hezbollah*, Wash. Post, Feb. 14, 2008 (“The world is a better place without this man in it. He was a coldblooded killer, a mass murderer and a terrorist responsible for countless innocent lives lost,” said State Department spokesman Sean McCormack), <http://www.washingtonpost.com/wp-dyn/content/article/2008/02/13/AR2008021300494.html>.

**I. AL QAEDA**

660. The United States has designated al Qaeda, and many of its affiliates, as an FTO, SDT, and SDGT.

661. Al Qaeda has been designated as a terrorist group by the following nations/organizations: Australia; Brazil; Canada; European Union; France; India; Iran; Ireland; Israel; Japan; Kazakhstan; NATO; Netherlands; New Zealand; Russian Federation; South Korea; Sweden; Switzerland; United Kingdom; and the United Nations Security Council.

662. The United Nations Security Council, in its Security Council Anti-Terrorism Frameworks, has considered terrorism a threat to international peace and security and has mandated the seizure and freezing of all funds and financial assets of individuals and groups associated with al Qaeda to ensure that no funds or financial assets be made available, directly or indirectly, to al Qaeda or any person or entity acting on its behalf:

- a) UNSC 1333 (12/19/2000);
- b) UNSC 1390 (1/2/2002);
- c) UNSC 1526 (1/30/2004);
- d) UNSC 1566 (10/18/2004);
- e) UNSC 1617 (7/29/2005);
- f) UNSC 1735 (12/22/2006);
- g) UNSC 1904 (12/17/2009); and
- h) UNSC 1989 (6/17/2011).

663. Al Qaeda is an international terrorist organization and not a “military force” and intentionally violates all core provisions of international humanitarian laws (laws of war), IHRL, and the ICC Statutes.

664. In addition to committing the terrorist attacks which are the subject of this lawsuit, al Qaeda intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings, intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions. For example:

- a) On February 23, 1998, Usama Bin Laden published a fatwa (ruling) evidencing his intention to violate international law, ordering all Muslims “to kill the Americans and their allies-civilians and military...in any country in which it is possible to do it....kill the Americans and plunder their money wherever and whenever they find it;”
- b) On August 7, 1998, al Qaeda, with the assistance and support of Iran and Sudan, bombed the United States embassies in Nairobi and Dar es Salaam, killing 224 and injuring over 5,000 diplomats and civilians;
- c) On September 11, 2001, al Qaeda, with assistance and support from Iran, launched attacks primarily against civilians in the United States;
- d) On January 23, 2002, al Qaeda kidnapped Wall Street Journal journalist Daniel Pearl in Karachi, Pakistan. al Qaeda leader Khalid Sheikh Mohammed (9-11 attack mastermind) confessed to having murdered Pearl saying, “I decapitated with my blessed right hand the head of the American Jew Daniel Pearl, in the city of Karachi, Pakistan.” Al Qaeda posted on the internet a video of the murder on February 23, 2002, under the caption The Slaughter of the Spy-Journalist the Jew Daniel Pearl. On May 16, Pearl’s severed head was found along with his body cut into ten pieces;
- e) On October 28, 2002, al Qaeda operatives Salem bin Suweid and Yasser Freihat (at the direction of Musab Abu al-Zarqawi and/or other al Qaeda senior leaders) murdered U.S. diplomat (USAID) Laurence Michael Foley Sr. outside of his home in Amman, Jordan;
- f) On March 11, 2004, al Qaeda killed 192 and injured over 2000 civilians in the bombings of commuter trains in Spain;
- g) On August 19, 2003, a suicide bomber driving a KAMAZ flatbed laden with military-grade munitions breached the gate at the U.N. headquarters in Iraq, detonated the cargo in front of the façade, and collapsed part of the three-story building. Among the 22 victims was the head of the U.N. mission in Iraq, and the director of the Council on Foreign Relations;

- h) In early September 2003, al Qaeda targeted and bombed the U.N. headquarters a second time to destroy the remnants of the mission;
- i) On August 29, 2003, al Qaeda bombed the Imam Ali mosque in Najaf, killing 95 Iraqi civilians and wounding hundreds of other civilians;
- j) In Ramadi, al Qaeda sawed off the heads of wounded Iraqi policemen at Ramadi General Hospital and of other civilians who supported coalition forces and used the seven-story hospital building to fire on coalition forces;
- k) On March 2, 2004, al Qaeda leader Abu Abdallah al Hassan Ben directed a series of suicide bombings in Karbala against Iraqi Shi'a Muslims celebrating the Shi'a holiday of Ashura, killing at least 178 and injuring at least 500 civilian Iraqi Shi'a Muslims;
- l) On or about April 10, 2004, al Qaeda kidnapped Nicholas Berg, an American civilian freelance radio-tower technician. On May 7, 2004, Musab Abu al-Zarqawi, leader of al Qaeda in Iraq, beheaded Nicholas Berg, and uploaded the video of the beheading to the internet on May 11th, with the caption "Abu Musab al-Zarqawi slaughters an American;"
- m) On May 30, 2004, Kim Sun-il, a translator was kidnapped and beheaded in a video released June 22, 2004;
- n) Abu Ayyub al-Masri (al Qaeda leader and head of the al Qaeda in Iraq wing following the death of al Zarqawi) killed Turkish truck driver hostage Murat Yuce (kidnapped in late July 2004). Al Qaeda filmed the murder and posted it on the internet on August 2, 2004;
- o) On September 16, 2004, al Qaeda kidnapped Americans Eugene Armstrong and Jack Hensley, and British engineer Ken Bigley, all civilian contractors for the construction firm Gulf Supplies Commercial Services. Al Qaeda threatened to kill the hostages within 48 hours unless women Iraqi prisoners held by coalition forces were released. Abu Musab al-Zarqawi personally beheaded Armstrong on September 20th, when the deadline expired. Hensley was beheaded 24 hours later and Bigley two weeks later. Al Qaeda filmed and posted on the internet all of the beheadings;
- p) At the end of October 2004, al Qaeda kidnapped Japanese citizen Shosei Koda, giving Japan 48 hours to withdraw troops or Koda's fate would be "the same as that of his predecessors, [Nicholas] Berg and [Kenneth] Bigley and other infidels." Koda was beheaded when Japan refused to comply and his dismembered body was found on October 30, 2004;

- q) On December 2004, Al-Jazeera broadcasted an audiotape of Usama bin Laden endorsing al-Zarqawi as his deputy in Iraq and called for a boycott of the elections;
- r) On January 2005, al-Zarqawi vowed to kill candidates and voters in the Iraqi elections, claimed responsibility for the assassination of Baghdad governor Ali al-Haidri as well as a number of attacks on polling day;
- s) May 2005, al-Zarqawi sent an audiotape report to Usama bin Laden, assuring him that he is in good health;
- t) August 2005 al Qaeda vowed to kill anyone involved in drafting Iraq's new constitution;
- u) On November 9, 2005, Iraq-based al Qaeda suicide bombers Ali Hussein Ali al Shamari, Rawad Jassem Mohammed Abed and Safaa Mohammed Ali bombed the Grand Hyatt, SAS Radisson, and Days Inn hotels in Amman, Jordan, killing 62 civilians and injured 115;
- v) On February 22, 2006, al Qaeda bombed the al Askai mosque in Samarra, Iraq. Al Qaeda operative Abu Qudama confessed to perpetrating the attack along with Haitham al Badri, leader of one of the cells of al Qaeda in Iraq, along with four Saudi and two other Iraqi al Qaeda operatives;
- w) On April 24, 2009, two female suicide bombers attacked the revered Shi'ite Imam Moussa Al-Kadhim shrine in the Kadhimiya area of Baghdad as people gathered for Friday prayers, killing at least 60 (including 25 Iranian pilgrims and injuring 125 others);
- x) On April 23, 2010, a series of blasts near the main office of Shi'ite Muslim cleric Muqtada Al-Sadr and several Shi'ite mosques during Friday prayers killed 54 people and wounded 180 in Baghdad;
- y) On December 23, 2009, an IED attack on the Syrian Orthodox Church of St. Thomas in Mosul killed two persons and wounded six;
- z) On May 2, 2010, a Christian shopkeeper was killed and over one hundred students were injured when a convoy of school buses carrying Christian students was attacked after passing a security checkpoint on the outskirts of Mosul. The buses were transporting university students from the mainly Christian town of Hamdaniyah to Mosul. According to an Iraqi security official, the buses were escorted by Iraqi soldiers because of past threats and attacks against Christians in the area. A teenage student died later of her wounds;
- aa) On June 8, 2010, drive-by shooters riddled Hani Salim, a Christian shop owner, with 15 bullets in Kirkuk City;

- bb) On October 27, 2003, Zarqawi's group ushered in Ramadan with an explosion outside the International Committee of the Red Cross (ICRC) building killing two of its staff and ten Iraqi bystanders;
- cc) On November 1, 2009, a magnetic bomb stuck to a bus carrying passengers in central Karbala exploded, wounding at least 26 people;
- dd) On October 25, 2009, a suicide bomber killed 147 people and wounded more than 700 when two large truck bombs targeted the Ministry of Justice, housing many of the city's judges, lawyers, and court rooms, and, minutes later, targeted the Baghdad Provincial Council; and
- ee) On February 1, 2010, a female suicide bomber blew herself up in a crowd of Karbala-bound Shi'ite pilgrims in northeast Baghdad (41 killed, 106 wounded).

665. Al Qaeda leaders regard liberal Muslims, Shias, Sufis, and other sects as heretics and have attacked their mosques and gatherings; examples include the Yazidi community bombings, the Sadr City bombings, the Ashura massacre, and the April 2007 Baghdad bombings.

666. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services, and material support to al Qaeda.

**J. ANSAR AL SUNNA/ANSAR AL ISLAM**

667. The United States has designated AAI/Ansar al Sunna as an FTO and an SDGT.

668. AAI/Ansar al Sunna is an international terrorist organization and not a "military force" and intentionally violates all core provisions of international humanitarian laws (laws of war), IHRL, and the ICC Statutes

669. In addition to committing the terrorist attacks which are the subject of this lawsuit, Ansar Al Sunna/AI intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings, intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions. For example:

- a) The September 23, 2002 massacre at the village of Kheli Hama during which 42 police officers and Persmerga (military forces of Iraqi Kurdistan) were killed, tortured, and beheaded;
- b) The February 1, 2004 suicide bombing attacks on the offices of the two main Iraqi Kurdish political parties, the Kurdish Democratic Party, and the People's Union of Kurdistan party, killing at least 109 and injuring 130 civilians and elected officials;
- c) Kidnappings of numerous foreign civilians in Iraq in 2004, and the subsequent broadcasting of their beheadings via the internet;
- d) The June 27, 2004 video of a captured and blindfolded Marine. On July 3, 2004, Ansar al-Sunna claimed it had murdered hostage U.S. Marine Cpl. Wassef Ali Hassoun;
- e) At 7:15 on September 7, 2004, Ansar al-Islam kidnapped journalists Scott Taylor (Canadian freelancer) and Zeynep Tugrul (Turkish journalist for Turkish Sabah newspaper) holding them for 5 days and continually torturing, beating, and threatening them with execution before releasing them;
- f) Beheading of 12 civilian Nepalese hostages seized in Iraq (broadcast via video on the internet) claiming the hostages were “fighting the Muslims and serving Jews and the Christians” and “believing in Buddha as their God;” and
- g) The October 3, 2004 beheading of an Iraqi contractor and videotaped message threatened to kill other Iraqis working with Americans.

670. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services, and material support to Ansar al Sunna/AIAI.

**K. JAYSCH AL MAHDI**

671. JAM and its subsidiary, PDB, are international terrorist organizations and not “military forces” and intentionally violate all core provisions of international humanitarian laws (laws of war), IHRL, and the ICC Statute;

672. In addition to committing the terrorist attacks which are the subject of this lawsuit, Jaysch al Mahdi and PDB intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings, intended to terrorize, intimidate, and coerce civilian

populations, governments, and international institutions, and engage in widespread and systematic acts of mass murder, torture, ethnic cleansing, and genocide. For example:

- a) On April 2, 2004, in a sermon, Muqtada al Sadr issued what became known as the hawasim fatwa. Asserting the fundamental illegitimacy of Saddam Hussein's regime, he declared that any claims of ownership of goods or property were invalid – and that looters were entitled to the fruits of their plunder so long as they paid khums, a 20 percent religious tax on its value, to Sadrists officials;
- b) In a subsequent sermon, Muqtada proclaimed the September 11th attacks on the United States were “a miracle and blessing from God;”
- c) Muqtada further threatened that “[i]f America persists [in advocating for independent Sunni and Kurdish states], then it will cease to exist;”
- d) On July 9, 2006, JAM terrorists set up checkpoints across the Hay al Jihad neighborhood of Baghdad, asking drivers and passengers for identification. All Sunni males were taken to a bus and driven to a waste ground where over 50 civilian Sunni captives were murdered. In addition, JAM perpetrated numerous suicide bombings across Sunni neighborhoods in Baghdad from July 4-9, 2006, killing over 150 civilians as part of its widespread and systematic campaign of ethnic cleansing;
- e) In October 2006 in Samara, the group carried out an attack which resulted in 18 civilian casualties and 90 injuries;
- f) In March 2008 in Baghdad, JAM militants fired up to 30 mortar rounds and rockets at the International Green Zone, killing 14 civilians, including several children, one U.S. government contractor, wounding between 4 and 8 people, between 39-47 civilians, including several children; and
- g) On June 24, 2009, a JAM/PDB vehicle-borne IED resulted in 62 civilian deaths and 120 civilian casualties.

673. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services and material support to JAM.

#### **L. BADR ORGANIZATION**

674. Badr Organization is an international terrorist organization and not a “military force” and intentionally violates all core provisions of international humanitarian laws (laws of war), IHRL, and the ICC Statutes.

675. In addition to committing the terrorist attacks which are the subject of this lawsuit, Badr Organization intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings, intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions. For example:

- a) During at least 2003-2004, Badr Organization inserted numerous assassination teams from its bases in Iran who systematically murdered hundreds of Sunni former (Hors de combat) Iraqi army pilots and officers;
- b) On May 14, 2005, Ahmed al-Khafaji, a top leader in the Badr Organization, ordered the arrest and torture of retired (Hors de combat) Brigadier General Muhammed al-Azzawi and the torture and extrajudicial killing of his brother and 11 other civilians;
- c) On February 16, 2006, U.S. Maj Gen Joseph Peterson reported that U.S. forces had arrested 22 Iraqi policemen in northern Baghdad, members of Badr Organization death squad, who told U.S. soldiers they were taking a Sunni man away to be shot dead.<sup>33</sup> Hundreds of thousands of Sunni civilians have been kidnapped, tortured and killed by Badr Organization death squads;
- d) Badr Organization leader Hadi al-Amiri personally ordered attacks on up to 2,000 Iraqi Sunni civilians from 2004-2006 (when 2,000 were killed and an unknown number were wounded);
- e) Al-Amiri's preferred methods of killing allegedly involved using a power drill to pierce the skulls of his adversaries;<sup>34</sup>
- f) In July 2005, the morgue in Baghdad received 1,100 Sunni bodies, about 900 of which bore evidence of torture or summary execution;<sup>35</sup> and

---

<sup>33</sup> BBC News, *Iraq 'death squad caught in act'* (Feb. 16, 2006), [http://news.bbc.co.uk/2/hi/middle\\_east/4719252.stm](http://news.bbc.co.uk/2/hi/middle_east/4719252.stm).

<sup>34</sup> Loveday Morris, *Appointment of Iraq's new interior minister opens door to militia and Iranian influence*, Wash. Post, Oct. 18, 2014, [https://www.washingtonpost.com/world/appointment-of-iraqs-new-interior-minister-opens-door-to-militia-and-iranian-influence/2014/10/18/f6f2a347-d38c-4743-902a-254a169ca274\\_story.html?utm\\_term=.6ddc94d5364a](https://www.washingtonpost.com/world/appointment-of-iraqs-new-interior-minister-opens-door-to-militia-and-iranian-influence/2014/10/18/f6f2a347-d38c-4743-902a-254a169ca274_story.html?utm_term=.6ddc94d5364a).

<sup>35</sup> Andrew Buncombe & Patrick Cockburn, *Iraq's death squads: On the brink of civil war*, INDEPENDENT, Feb. 26, 2006, <http://www.independent.co.uk/news/world/middle-east/iraqs-death-squads-on-the-brink-of-civil-war-6108236.html>.

g) On November 13, 2005, there was a discovery of a detention center in Baghdad, run by Iraqi intelligence officials linked to Badr, where captives, mostly Sunni Arabs, were beaten, blindfolded, or subjected to electric shocks.<sup>36</sup>

676. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services, and material support to Badr Organization.

**M. KATA'IB HEZBOLLAH**

677. Kata'ib Hezbollah is an international terrorist organization and not a “military force” and intentionally violates all core provisions of international humanitarian laws (laws of war), IHRL, and the ICC Statutes.

678. The United States has designated Kata'ib Hezbollah as a FTO, a SDGT, and a Threat to Stabilizations Efforts in Iraq.

679. In addition to committing the terrorist attacks which are the subject of this lawsuit, Kata'ib Hezbollah intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings, intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions. For example:

- a) On June 4, 2008, Kata'ib Hezbollah killed 18 and injured 29 Iraqi civilians, destroying 19 homes;
- b) On November 29, 2008, KH launched a rocket attack, killing 2 U.N. contractors and injuring 15 other civilians;
- c) In July 2009, Kata'ib Hezbollah threatened the lives of Iraqi politicians and civilians who supported Iraq's political process;
- d) On July 2011, Kata'ib Hezbollah issued a statement threatening Kuwait and the workers who were building a port near Kuwait's border with Iraq;

---

<sup>36</sup> Council on Foreign Relations, *Shiite Militias and Iraq's Security Forces* (Nov. 30, 2005), <https://www.cfr.org/backgrounder/shiite-militias-and-iraqs-security-forces>.

- e) In June 2014, Human Rights Watch found Kata'ib Hezbollah and Asa'ib Ahl al-Haq and other Shite terrorist groups had carried out “indiscriminate attacks in civilian areas,” and had also conducted kidnapping operations and carried out summary executions of Sunnis in the towns of Buhriz, Mada'in, al-Heetawy, and other towns;
- f) In November 2008, Kata'ib Hezbollah threatened to attack the Iraq government if it signed the security agreement with the United States; and
- g) Kata'ib Hezbollah kidnapped 18 Turkish construction workers in Baghdad, in September 2015.

680. Kata'ib Hezbollah committed a systematic and widespread campaign of ethnic cleansing, terrorism, torture, extrajudicial killings, kidnappings, and mayhem against Sunni civilians across areas of Iraq formerly held by the Islamic State. For example:

- a) On July 5, 2016, Zeid Ra'ad Al Hussein, United Nations High Commissioner for Human Rights, said more than 700 Sunni men and boys (out of the 1,500 Sunni males over the age of 15 taken captive by Kata'ib Hezbollah) are missing two months after the Islamic State was vanquished from Fallujah. The men and boys were shot, beaten with rubber hoses, and in at least 4 cases, beheaded. At least 69 have been summarily executed or tortured to death while in the initial custody of Kata'ib Hezbollah;
- b) On May 27, 2016, approximately 90 males aged 15 and older were taken and have not been located since;
- c) On May 29, 2016, twenty men from a group of fleeing men, women, and children were killed. Another group of families, raising white flags, surrendered. The males were separated and 17 of them were then summarily shot and killed; and
- d) On June 3, 2016 Kata'ib Hezbollah rounded up 1,500 Sunnis males, aged 15 and older from the town of Saqlawiya, and moved them into warehouses and an Iraqi base called Camp Tariq. The survivors described being crammed into small rooms and halls and denied food and water, straining to breathe in the stifling heat. Kata'ib Hezbollah terrorists, using sticks, pipes, and hoses, beat the detainees and declared that they were taking revenge for Camp Speicher – a June 2014 massacre by the Islamic State of 1,566 Shi'ite and other non-Sunni Air Force cadets. A 47-year-old survivor described how he watched his 17-year-old son repeatedly beaten and the corpses of 15 other men carried off who appeared to have been beaten to death. The man was one of the 605 survivors released on June 5, 2016. His son was not among them, he said; the boy hasn't been seen since.

681. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services, and material support to Kata'ib Hezbollah.

**N. ASA'IB AHL AL-HAQ**

682. Asa'ib Ahl al-Haq is an international terrorist organization and not a "military force" and intentionally violates all core provisions of international humanitarian laws (laws of war), IHRL, and the ICC Statutes.

683. In addition to committing the terrorist attacks which are the subject of this lawsuit, Asa'ib Ahl al-Haq intentionally targeted civilians, diplomats, hospitals, religious institutions, military personnel, and non-combatants alike, and perpetrated acts of mass murder, assassinations, and kidnappings, intended to terrorize, intimidate, and coerce civilian populations, governments, and international institutions. For example:

- a) Asa'ib Ahl al-Haq has launched over 6,000 attacks in Iraq, thousands of which targeted civilians, including the October 3, 2007 attempted assassination of Gen. Edward Pierzyk, the Polish ambassador to Iraq. Three bombs struck the embassy's three-car convoy (all bearing Polish flags) killing three members of the Polish embassy, injuring the ambassador and 8 other civilians and 3 soldiers.
- b) In May 2007, Asa'ib Ahl al-Haq kidnapped Peter Moore, a British IT expert, along with four bodyguards from a government building in Baghdad. Peter Moore was beaten on a near-daily basis and the bodyguards were tortured and murdered.
- c) In February 2010, Asa'ib Ahl al-Haq kidnapped Department of Defense civilian employee Issa T. Salomi who was released in March 2010 in exchange for the release of 4 AAH terrorists held in Iraqi custody.

684. Defendants knew, or were deliberately indifferent to, the fact Iran provided funding, financial services and material support to Asa'ib Ahl al-Haq.

**V. THE DEFENDANTS**

685. Plaintiffs assert causes of action against Defendants and Defendant Bank Saderat.

686. During the Relevant Period, each Defendant was and is a "United States person" under 18 U.S.C. § 2332d and 31 C.F.R. § 560.314. Section 2332d defines "United States person"

to mean any: “(D) any person in the United States.” 18 U.S.C. § 2331(3) provides that a “person” is “any individual or entity capable of holding a legal or beneficial interest in property.” Each of the defendants are entities, and operated branches in the United States.

687. During the Relevant Period, Defendants Deutsche Bank AG; HSBC Bank USA, N.A.; HSBC Holdings; HSBC Bank Plc; HSBC Bank Middle East Limited; HSBC North America; Commerzbank AG; Commerzbank AG, New York; Barclays Bank Plc; BNP Paribas S.A.; Standard Chartered Bank; Royal Bank of Scotland N.V.; Royal Bank of Scotland Plc; Crédit Agricole S.A.; Crédit Agricole Corporate Investment Bank; Credit Suisse A.G.; and Bank Saderat Plc conspired with one or more of their codefendants and/or Bank Markazi; and/or Bank Melli Iran; and/or Melli Bank Plc; and/or Bank Mellat; and/or Bank Tejarat; Bank Refah; and/or Bank Sepah; and/or the IRISL; and/or Mahan Air; and/or the National Iranian Oil Company (“NIOC”); and/or the IRGC; and/or the IRGC-QF; and/or Hezbollah; Kahtum, and/or others unknown to your plaintiffs, to defeat the economic sanctions imposed by: OFAC, the United Nations (U.N.) and the European Union (E.U.) which were designed to influence Iran’s central government to stop sponsoring terrorism. Court and agency documents, including criminal information, deferred prosecution agreements, consent orders, guilty pleas, executive orders, and settlement agreements, detail the actions of Defendants as set forth herein, and those documents are incorporated herein in full as if reproduced in this complaint.

688. Defendants are sophisticated financial institutions that routinely conduct business in the United States, including at the times giving rise to this cause of action.

689. Defendants are required to monitor, detect, and disclose transactions intended to circumvent U.S. sanctions to U.S. regulators, law enforcement, and counter-terrorism agencies, as well as report any instance of noncompliance with these requirements.

690. Among some of the duties owed by Defendants are the following:

- a) Maintain an effective AML program – Title 31, United States Code, Section 5318(h) and regulations issued thereunder;
- b) Conduct and maintain due diligence on correspondent bank accounts held on behalf of foreign persons – Title 31, United States Code, Section 5318(i) and regulations issued thereunder;
- c) Abide by the Trading with the Enemy Act, Title 50, United States Code Appendix, Sections 3, 5, 16, and regulations issued thereunder;
- d) Abide by the International Emergency Economic Powers Act, Title 50, United States Code (“IEEPA”), Sections 1702 and 1705, and regulations issued thereunder;
- e) Abide by the Anti-Terrorism Act of 2001(ATA); and
- f) Abide by Executive Orders 13067 (Nov. 3, 1997) and 13412 (Oct. 13, 2006) and related regulations promulgated by OFAC.

691. Under Executive Order 13067 (November. 3, 1997) and Executive Order 13412 (Oct. 13, 2006) and related regulations promulgated by OFAC pursuant to IEEPA, it is unlawful to export goods and services from the United States, including U.S. financial services, to Iran without a license from OFAC. Under these Executive Orders and regulations, virtually all trade and investment activities with Iran involving the U.S. financial system, including the processing of USD transactions through the United States, were prohibited.

692. Instead of performing the functions required of them, Defendants supported Iran and its Agents and Proxies by deliberately evading U.S. economic sanctions, conducting illicit trade-finance transactions, and disguising financial payments to and from USD-denominated accounts.

693. Defendants knew or were deliberately and/or recklessly indifferent to the fact with their assistance, Iran was able to provide material support and resources to designated FTOs in violation of 18 U.S.C. §§ 2339A and 2339B(a)(1).

694. Further, having reasonable cause to know that Iran was supporting international terrorism, Defendants engaged in financial transactions with Iran and/or its Agents and Proxies in violation of 18 U.S.C. § 2332d.

695. Moreover, Defendants knew or were deliberately and/or recklessly indifferent to the fact they were concealing the financing of terrorism in violation of 18 U.S.C. § 2339C.

696. These transfers not only overlapped with the Terrorist Attacks that caused Plaintiffs' injuries, but also occurred at a time when Defendants knew or were deliberately indifferent to the fact funds it transferred on behalf of the Iranian Agents and Proxies were being used to support the Terrorist Groups responsible for the Terrorist Attacks that injured or killed Plaintiffs.

697. In this action, the claims of all Plaintiffs arise, at least in part, from the transactions facilitated through Defendants in the United States. Because the USD transfers facilitated and completed through Defendants on behalf and at the request of Iran and Defendant Bank Saderat, were a substantial part of the unlawful conduct perpetrated by Defendants, the Court may exercise jurisdiction with respect to all of Plaintiffs' claims.

698. The repeated use of correspondent accounts in New York to effectuate these illegal fund transfers constitute a course of dealing by the Defendants in the U.S. Each fund transfer referenced herein was effectuated by Defendants in the United States at the request of Defendant Bank Saderat and Iran or Iran's proxies, as each such transfer of funds was for the benefit of the Terrorist Groups being provided with material support that allowed them to perpetrate the acts of international terrorism identified herein. Thus, the Corporate Defendants have purposefully availed themselves of the laws of New York's transparent banking system and the predictable jurisdictional and commercial laws of New York and the United States.

699. Defendants deliberately and repeatedly used a United States account to support the same terrorist organizations which perpetrated the Terrorist Attacks.

700. A sufficient and articulable nexus exists which demonstrates a substantial relationship between Plaintiffs' claims and Defendants' transactions in the State of New York. To be certain, as it relates to Plaintiffs' claims, Defendants utilized correspondent accounts in the State of New York to facilitate the clearing of USD transfers requested by the Iranian Agents and Proxies who maintained bank accounts for the benefit of the Terrorist Groups that were responsible for the Terrorist Attacks, and such wire transfers violated the very statutes at issue in this litigation—namely the IEEPA (18 U.S.C. § 371), the Bank Secrecy Act (31 U.S.C. § 5318, 31 U.S.C. § 5322, failing to report suspicious activity, and failing to establish due diligence for foreign correspondent accounts in violation of 31 U.S.C. §§ 5318, 5322.

701. In executing these fund transfers, Defendants used New York's banking system to affect the very financial support that is the basis of Plaintiffs' claims.

702. Due to the conduct complained of herein, each Defendant either plead guilty to felony charges under U.S. and New York state laws or entered into Deferred Prosecution Agreements ("DPA") with the U.S. and New York state governments.

**A. DEUTSCHE BANK AG**

703. Deutsche Bank AG ("DB") is a large international bank with over 98,000 employees and over \$1.6 trillion dollars in total assets. DB is headquartered in Taunusanlage 12, Frankfurt, Germany.

704. DB operates a branch in New York, New York ("DB New York") through which it conducts correspondent banking services and USD clearing activities for its international branches and customers.

705. DB may be properly served through its agents located in Deutsche Bank AG, 60 Wall Street, New York, NY 10005 or its registered agent CT Corporation System 1200 South Pine Island Road, Plantation, FL 33324.

706. This Court may exercise personal jurisdiction over DB pursuant to Fed. R. Civ. P. 4(k)(1)(C), because the DB Defendants can be served in the United States pursuant to the ATA.

707. Specifically, DB conducted business in the United States through its offices in New York, California, Texas, Florida, Illinois, and Washington, D.C., among others.

708. In addition to the New York office, DB operates over thirty banking locations throughout the United States in 18 different states.

709. During the Relevant Period, DB transferred money to certain charitable organizations that were actually fronts for Iran.

710. DB deliberately and repeatedly (**more than 27,000 times**) used a New York account to support the same terrorist organizations who perpetrated the Terrorist Attacks.<sup>37</sup>

711. Although the transfers at issue vary in time and location to a degree, such transfers substantively constitute a single course of conduct by DB that entailed violations of U.S. law in the same manner with respect to all Plaintiffs' claims.

## **B. THE HSBC DEFENDANTS**

712. The HSBC Defendants comprise financial institutions throughout the world that are owned by various intermediate holding companies, and ultimately and indirectly, Defendants HSBC Holdings.

713. HSBC Holdings, HSBC North America, HSBC-US, HSBC-London, and HBME are collectively referred to herein as "the HSBC Defendants."

---

<sup>37</sup> See Section VII(B)(2) for more detail regarding DB's involvement in the Conspiracy.

714. The HSBC Defendants routinely conducted business in the State of New York through a correspondent account it maintained at that branch, utilizing that account to clear USD transfers requested by its customers.

715. This Court may exercise personal jurisdiction over the HSBC Defendants pursuant to Fed. R. Civ. P. 4(k)(1)(C).

716. The key U.S. affiliate is HSBC Bank USA N.A. (“HSBC-US”). HSBC-US operates more than 470 bank branches throughout the United States, manages assets totaling about \$200 billion, and serves around 3.8 million customers. It holds a national bank charter, and its primary regulator is the U.S. Office of the Comptroller of the Currency, which is part of the U.S. Treasury Department. HSBC-US is headquartered in McLean, Virginia, but has its principal office in New York City. HSBC acquired its U.S. presence by purchasing several U.S. financial institutions, including Marine Midland Bank and Republic National Bank of New York.

717. Among other entities, the Group owns HSBC Overseas Holdings (UK) Ltd. (“HSBC Overseas Holdings”), which oversees its operations in the United States and Canada. HSBC Overseas Holdings owns, in turn, HSBC-North America, one of the ten largest bank holding companies in the United States. HSBC North America has assets of about \$345 billion, is headquartered in New York City, and is overseen by the Federal Reserve. Through various subsidiaries, HSBC North America owns three key HSBC financial institutions in the United States: HSBC-US; HSBC Securities (USA) Inc.; and HSBC Finance Corporation. HSBC-US operates more than 470 bank branches throughout the United States, manages assets totaling about \$210 billion, and serves around 4 million customers. It holds a national bank charter and its primary regulator is the Office of the Comptroller of the Currency, which is part of the U.S. Treasury Department. Because it holds insured deposits, its secondary regulator is the Federal

Deposit Insurance Corporation. HSBC-US is the principal subsidiary of HSBC USA Inc., a bank holding company which is a wholly-owned subsidiary of HSBC North America. HSBC-US is headquartered in McLean, Virginia, and has its principal office in New York City.

718. The HSBC-US “Global Banking and Markets” line of business, with offices in more than 60 countries, provides a wide range of “tailored financial solutions” to major government, corporate, and institutional clients. This line of business includes an extensive network of correspondent banking relationships, in which HSBC-US provides banks from other countries with USD accounts to transact business in the United States. Due to its affiliates in over 80 countries, HSBC is one of the largest providers of correspondent banking services in the world.

719. In 2010, HSBC-US had about 2,400 correspondent customers, including more than 80 HSBC affiliates. Among other services, HSBC provides financial institution clients with access to the U.S. financial system by handling international wire transfers, clearing a variety of USD instruments, including travelers checks and money orders, and providing foreign exchange services. HSBC-US Payment and Cash Management is a key banking division, located in New York, that supports HSBC-US’ correspondent relationships.

720. In addition, as part of this line of business, until 2010, HSBC-US housed the Global Banknotes Department, which used offices in New York City, London, Hong Kong, and elsewhere to buy, sell, and ship large amounts of physical USD. The Banknotes Department derived its income from the trading, transportation, and storage of bulk cash, doing business primarily with other banks and currency exchange businesses, but also with HSBC affiliates. In addition, for a number of years, HSBC-US held a contract with the U.S. Federal Reserve Bank of New York (“FRBNY”) to operate U.S. currency vaults in several cities around the world to assist

in the physical distribution of USD to central banks, large commercial banks, and businesses involved with currency exchange. In June 2010, however, HSBC-US exited the wholesale U.S. banknotes line of business.<sup>38</sup>

### **1. HSBC Holdings Plc**

721. HSBC Holdings Plc (“HSBC Holdings”) is a public limited company, organized under the laws of the United Kingdom with its principal place of business there.

722. HSBC Holdings is the ultimate parent company of one of the world’s largest banking and financial services groups with approximately 6,900 offices in over 80 countries.

723. HSBC Holdings directly or indirectly owns, *inter alia*, HSBC Bank Plc, HSBC Bank Middle East Limited, HSBC Bank USA, N.A., and HSBC North America

724. HSBC Holdings is listed on the New York Stock Exchange, London Stock Exchange and Hong Kong Stock Exchange.

725. HSBC Holdings Plc may be properly served in accordance with the Hague Convention at its agent located at 8 Canada Square, London E14 5HQ, England.

726. HSBC Holdings sent or cleared USD payments through the U.S., including clearing done through U.S. subsidiaries.

### **2. HSBC North America Holdings, Inc.**

727. HSBC North America, is a Delaware corporation and is an indirect subsidiary of HSBC Holdings.

728. According to fact sheets published on HSBC’s official website, HSBC North America Holdings Inc. is headquartered in New York City and Illinois.

---

<sup>38</sup> United States Senate Permanent Subcommittee on Investigations, *U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Case Financing: HSBC Case History* (Jul. 17, 2012), <https://www.hsgac.senate.gov/subcommittees/investigations/hearings/us-vulnerabilities-to-money-laundering-drugs-and-terrorist-financing-hsbc-case-history>.

729. HSBC North America is the holding company for HSBC Holding Plc's operations in the United States.

730. HSBC North America's businesses serve customers in retail banking and wealth management, commercial banking, private banking, and global banking and markets.

731. HSBC North America may be properly served through its registered agent, The Corporation Trust Company, Corporation Trust Center, 1209 Orange Street, Wilmington, DE 19801.

### **3. HSBC Bank USA, N.A.**

732. HSBC-US is a federally chartered banking institution under the National Bank Act (12 U.S.C. ch. 2 et seq.), is registered, organized, or incorporated in New York.

733. HSBC-US is the principal subsidiary of HSBC USA Inc., a wholly-owned subsidiary of HSBC North America. HSBC-US is a Member of the Federal Deposit Insurance Company.

734. HSBC-US operates more than 240 bank branches throughout the United States, including over 145 branches in New York, as well as branches in: California; Connecticut; Delaware; Washington, D.C.; Florida; Maryland; New Jersey; Pennsylvania; Virginia; and Washington State.

735. The Department of the Treasury, Office of the Comptroller of the Currency is HSBC Bank USA's primary regulator.

736. HSBC Bank USA, N.A. may be properly served through its registered agent, The Corporation Trust, Incorporated, 2405 York Road, Suite 201, Lutherville Timonium, MD 21093.

#### **4. HSBC Bank Plc**

737. HSBC Bank Plc (“HSBC-London”) often referred to internally by members of HSBC Group as “HBEU”) is a financial institution registered under the laws of England and Wales. It operates nearly 1,000 branches in the United Kingdom, Isle of Man, and the Channel Islands.

738. HSBC-London is one of the four major clearing banks in the United Kingdom and is a wholly owned subsidiary of HSBC Holdings.

739. HSBC-London may be properly served in accordance with the Hague Convention, at its registered office at 8 Canada Square, London E14 5HQ, England or its authorized agent at HSBC-London, 11 West 39th Street, New York, New York 10018.

#### **5. HSBC Bank Middle East Limited**

740. HSBC Bank Middle East Limited (often referred to internally by members of HSBC Group as “HBME”), is a financial institution headquartered in Dubai, United Arab Emirates (“UAE”), and registered under the laws of the Jersey Channel Islands.

741. HBME may be properly served in accordance with the Hague Convention through its agent located at Unit GV08-1st Floor-Full Floor, L Gate Village Building 8 Dubai AE.

742. HBME sent or cleared USD payments through the U.S., including clearing done through U.S. subsidiaries.

743. HBME maintained correspondent bank accounts at financial institutions in New York and utilized the respective account to effectuate a significant number of wire transfers on behalf of Iran, its Agents and Proxies, and the Terrorist Groups.<sup>39</sup>

---

<sup>39</sup> See Section VII(B)(3) for more detail regarding the HSBC Defendants’ involvement in the Conspiracy.

**C. COMMERZBANK AG AND COMMERZBANK AG, NEW YORK BRANCH**

744. Defendant Commerzbank AG (“Commerzbank”) is a financial services company formed under the laws of Germany and headquartered in Frankfurt, Germany and has over 1,200 branches in Germany, alone.

745. Commerzbank has locations in 23 countries, including a representative office in Tehran, Iran and a New York branch licensed by the State of New York since 1967.

746. Commerzbank AG, New York Branch (“Commerzbank New York”) is headquartered in New York, New York.

747. Commerzbank is listed on stock exchanges in Germany, London, and Switzerland.

748. Additionally, this Court may exercise personal jurisdiction over Defendant Commerzbank pursuant to Fed. R. Civ. P. 4(k)(1)(C).

749. Commerzbank and Commerzbank New York may be properly served through their agents for service at their offices located at 225 Liberty Street, New York, New York 10281.

**D. BARCLAYS BANK PLC**

750. Defendant Barclays Bank Plc (“Barclays”) is a global financial services provider headquartered in London, England. Defendant is a wholly owned subsidiary of Barclays Plc, a public limited liability company organized under the laws of England and Wales. This complaint refers to the subsidiary company.

751. Barclays maintains an extensive network of twelve corporate and investment banking branches and subsidiaries in the United States spread throughout Georgia, Massachusetts, Illinois, Texas, California, Florida, New York, Washington, and Washington D.C.

752. Barclays lists its corporate banking office in the United States as its New York city branch and this branch functioned as its primary clearance house for USD transactions for itself, its affiliates and clients.

753. During the Relevant Period, Barclays maintained a New York branch that functioned as the primary USD clearer for all of Barclays, its affiliates, and its customers.

754. Barclays' provision of USD transactions is an important part of its full service international business banking business model.

755. Barclays has operated in and been licensed and regulated by the State of New York since 1963.

756. Barclays New York branch has more than 500 employees and total assets in excess of \$36 billion.

757. Additionally, this Court may exercise personal jurisdiction over Defendant Barclays pursuant to Fed. R. Civ. P. 4(k)(1)(C).

758. Defendant Barclays resides, is found, or has an agent in New York, Nevada, New Jersey, Delaware, Ohio, Texas, Maine, Georgia, Massachusetts, Illinois, California, Florida, Washington and Washington, D.C.

759. Defendant Barclays may be properly served through its agent for service at its offices located at 745 7th Avenue, New York, New York 10019.

**E. BNP PARIBAS S.A.**

760. Defendant BNP Paribas S.A. ("BNP") is the largest bank in France and is one of the five largest banks in the world by total assets. BNP has branches all through the world, including the United States.

761. Its operations in the United States are headquartered in New York, with branch offices in California, Hawaii, Texas, Illinois, Pennsylvania, and New Jersey.

762. Defendant BNP may be properly served through its General Counsel, Peter Cooke, at 787 7th Avenue, New York, NY 10019 and in accordance with the Hague Convention at its offices located at 16, boulevard des Italiens, Paris, Ile-de-France, France.

763. Defendant BNP routinely conducted business in the state of New York through a correspondent account it maintained at that branch, utilizing that account to clear USD transfers requested by its customers.

764. Such transfers substantively constitute a single course of conduct by Defendant BNP that entailed violations of U.S. law in the same manner with respect to all Plaintiffs' claims.<sup>40</sup>

765. Additionally, this Court may exercise personal jurisdiction over Defendants BNP pursuant to Fed. R. Civ. P. 4(k)(1)(C).

766. Defendant BNP resides, is found, or has an agent in New York, New Jersey, California, Illinois, Texas, California, and Pennsylvania.

#### **F. STANDARD CHARTERED BANK**

767. Defendant Standard Chartered Bank ("SCB") is one of the world's largest international banks, with over 1,700 branches, offices, and outlets in more than 70 countries. SCB operates principally in Asia, Africa, and the Middle East, but maintains its principal place of business in London.

768. SCB operates a foreign branch in New York City, New York. This branch provides wholesale banking services, primarily clearing for international wire payments at approximately \$195 Billion per day.

---

<sup>40</sup> See Section VII(B)(6) for more detail regarding BNP's involvement in the Conspiracy.

769. Additionally, this Court may exercise personal jurisdiction over Defendant SCB pursuant to Fed. R. Civ. P. 4(k)(1)(C).

770. Defendant SCB resides, is found, or has an agent in New York, New Jersey, Texas, California, Florida, and Washington D.C.

771. SCB may be properly served through its registered agent C T Corporation System, 818 W 7th Street, Ste. 930, Los Angeles, CA 90017 or through its agent authorized to receive process at its offices located at 1095 Avenue of the Americas New York, New York 10036.

**G. ROYAL BANK OF SCOTLAND N.V. AND ROYAL BANK OF SCOTLAND PLC**

772. The Royal Bank of Scotland Plc, (“RBS Plc”) is an international banking and financial services institution and a wholly owned subsidiary of The Royal Bank of Scotland Group Plc (“RBS Group”).

773. At all relevant times, RBS Plc was licensed by the New York Department of Financial Services (“DFS”) to operate as a foreign bank branch in New York.

774. In October 2007, a consortium consisting of Fortis, the RBS Group, and Banco Santander, acquired ABN Amro Holding N.V., the parent company of ABN Amro Bank N.V., using the acquisition vehicle, RBS Holdings.

775. The former ABN Amro Bank N.V. subsequently underwent a restructuring process to transfer its Dutch State-acquired businesses and activities out of the existing ABN Amro Group. To do so, the relevant Dutch State-acquired businesses were first transferred to a new legal entity owned by ABN Amro Holding N.V.

776. On February 5, 2010, through a statutory demerger process, the former ABN Amro Bank N.V. was renamed Royal Bank of Scotland, N.V. (“RBS N.V.”)

777. Ultimately, RBS Group acquired ABN Amro Holding N.V. As such, RBS Group acquired the New York and Chicago branches of ABN Amro Bank N.V. and began integrating certain business lines handled by these branches into its other U.S. operations.

778. At all times relevant to this Complaint and through 2015, RBS Group conducted banking operations in the United States through branches of RBS Plc in New York, New York and Stamford, Connecticut, and branches of RBS N.V. in New York (Royal Bank of Scotland N.V., (New York)) and Chicago, Illinois (Royal Bank of Scotland N.V., (Chicago)).

779. RBS Plc and RBS N.V. are collectively referred to herein as “RBS.”

780. RBS currently provides banking services and products in the United States through its offices in Stamford, Connecticut.

781. RBS is subject to supervision and regulation by a variety of U.S. state and federal regulatory agencies, including the Connecticut Department of Banking and the Federal Reserve.

782. RBS N.V. may be properly served through its agent for service at 600 Washington Blvd., Stamford, CT 06901.

783. RBS Plc may be properly served through its registered agent, Corporation Service Company which will do business in California as CSC – Lawyers Incorporating Service, 2710 Gateway Oaks Drive, Suite 150N, Sacramento, CA 95833.

784. RBS Group may be properly served through its agent for service at 600 Washington Blvd., Stamford, CT 06901.

785. This Court may exercise personal jurisdiction over RBS pursuant to Fed. R. Civ. P. 4(k)(1)(C), because RBS can be served in the United States pursuant to the ATA.

786. Defendant RBS resides, is found, or has an agent in the United States, specifically in Connecticut.

787. “As detailed in a DFS consent order, employees at RBS acted to conceal the identity of sanctioned clients by various means, including implementing formal procedures to strip out identifying data from payment messages. This misconduct represented threatened the safety and soundness of RBS and violated New York Law, including the obstruction of governmental administration, failure to report crimes and misconduct, offering false instruments for filing, and falsifying business records. The Bank agrees the conduct at issue involved more than 3,500 transactions through New York correspondent banks valued at approximately \$523 million.”<sup>41</sup>, <sup>42</sup>

788. “From at least 2002 to 2011, RBS conducted more than 3,500 transactions valued at approximately \$523 million through New York correspondent banks involving Sudanese and Iranian customers and beneficiaries, including a number of entities on the SDN list of OFAC...”<sup>43</sup>

789. RBS routinely conducted business in the state of New York through a correspondent account it maintained at that branch, utilizing that account to clear USD transfers requested by its customers.

#### **H. CRÉDIT AGRICOLE S.A. AND CRÉDIT AGRICOLE CORPORATE & INVESTMENT BANK**

790. Defendant Crédit Agricole S.A. (“CASA”) is the largest retail banking group in France and is headquartered in Montrouge, France. Defendant Crédit Agricole Corporate and

---

<sup>41</sup> New York State Dep’t of Financial Services, *Cuomo Administration Announces RBS to Pay \$100 Million for Violations of Law Involving Transactions with Iran, Sudan, Other Regimes* (Dec. 11, 2013), <http://www.dfs.ny.gov/about/press/pr131211.htm>.

<sup>42</sup> See Section VII(B)(8) for more detail regarding RBS’ involvement in the Conspiracy.

<sup>43</sup> New York State Dep’t of Financial Services, *In re Matter of THE ROYAL BANK OF SCOTLAND PLC, Consent Order Under New York Banking Law § 44*, [http://www.dfs.ny.gov/about/ea/ea131211\\_rbs.pdf](http://www.dfs.ny.gov/about/ea/ea131211_rbs.pdf) (last visited Oct. 14, 2017).

Investment Bank (“CACIB”) have a number of subsidiaries and affiliated entities involved in transactions with Iran and Iranian entities that violated United States law.

791. In June of 2003, CASA purchased Crédit Lyonnais (“CL”). CL owned a subsidiary named Credit Lyonnais (Suisse) S.A. (“CLS”). CLS then merged with a CACIB subsidiary in Switzerland, Crédit Agricole Indosuez (Suisse) S.A. (“CAIS”). The resulting entity became Crédit Agricole (Suisse) S.A.

792. CACIB is the result of a 2004 transfer of the corporate and investment banking operations of CL to another CASA subsidiary, Crédit Agricole Indosuez. CACIB initially operated as “Caylon.” In 2010, it began operating under its current name, CACIB. Hereinafter, regardless of whether the entity was operating under the name Caylon or CACIB, the entity is identified as CACIB.

793. CACIB’s New York branch is subject to oversight and regulation by the Board of Governors of the U.S. Federal Reserve System and the New York State Banking Department.

794. Additionally, this Court may exercise personal jurisdiction over Defendants CASA and CACIB pursuant to Fed. R. Civ. P. 4(k)(1)(C).

795. Defendant CACIB resides, is found, or has an agent in New York.

796. Defendants CASA and CACIB transferred money to certain charitable organizations that were actually Iranian Agents and/or Proxies.

797. Defendant CASA may be properly served through in accordance with the Hague Convention by and through its agent for service, at its headquarters located at 50 avenue Jean Jaurès 92 120 Montrouge, France, or its agent for service at its offices located at 1301 Avenue of the Americas, New York, New York 10019.

798. Defendant CACIB may be properly served through its registered agent Corporation Company of Miami, 200 S. Biscayne Blvd., Ste. 4100 (GR), Miami, FL 33131.

799. Defendants CASA and CACIB routinely conducted business in the State of New York through a correspondent account it maintained at that branch, utilizing that account to clear USD transfers requested by its customers.

800. Such transfers substantively constitute a single course of conduct by Defendants CASA and CACIB that entailed violations of U.S. laws in the same manner with respect to all Plaintiffs' claims.<sup>44</sup>

801. Further, Defendants CASA and CACIB knew that such transfers were funding the terrorists responsible for the Terrorist Attacks.

### **I. CREDIT SUISSE AG**

802. Defendant Credit Suisse AG ("Credit Suisse") is a financial services company headquartered in Zurich, Switzerland. Credit Suisse serves clients worldwide and, at the time of the events giving rise to this action, Defendant Credit Suisse conducted business in the United States, and continues to do business in the United States.

803. Specifically, (according to its official corporate website), Defendant Credit Suisse conducts business in the United States through numerous offices and branches, including offices/branches in Atlanta, Georgia; Birmingham, Michigan; Boston, Massachusetts; Chicago, Illinois (2 offices/branches); Dallas, Texas; Houston, Texas; Los Angeles, California; Montgomery, Alabama; New York, New York; Northbrook, Illinois; Portland; Oregon; Raleigh, North Carolina; San Diego, California; San Francisco, California (2 offices/branches); Washington, D.C.; West Conshohocken, Pennsylvania; and West Palm Beach, Florida.

---

<sup>44</sup> See Section VII(B)(10) for more detail regarding Credit Suisse's involvement in the Conspiracy.

804. Defendant Credit Suisse's United States headquarters is located at 11 Madison Avenue, New York, New York.

805. In addition to its direct operations in the United States, Defendant Credit Suisse further transacts business in the United States through certain subsidiaries, including Credit Suisse Holdings (USA) Inc., Credit Suisse Securities, (USA) LLC, and Credit Suisse (USA), Inc.

806. Defendant Credit Suisse's operations in the United States are subject to oversight and regulation by the Board of Governors of the U.S. Federal Reserve System, the Securities and Exchange Commission, and various state banking regulatory agencies. Its New York branch is licensed by the New York Superintendent of Financial Services, examined by the DFS, and subject to laws and regulations applicable to a foreign bank operating a New York branch.

807. Defendant Credit Suisse may be properly served through its registered agent, Corporation Service Company located at 80 State Street, Albany, New York 12207-2543 or through its agent for service at its Principal Executive Office located at 11 Madison Avenue, New York, New York 10010 .

808. During the relevant times described in this Complaint and as part of its business in the United States, Defendant Credit Suisse utilized its United States' offices/branches and correspondent banks to transfer money to certain charitable organizations that were actually Iranian Agents and/or Proxies, which money Defendants Credit Suisse knew was being used to fund the Terrorist Attacks that are the subject of this Complaint. Beginning in the mid-1990s and continuing through 2006, Credit Suisse systematically violated both U.S. and New York State laws by moving hundreds of millions of dollars illegally through the U.S. financial system on behalf of entities subject to U.S. economic sanctions.

809. Credit Suisse engaged in this criminal conduct by: (a) removing or falsifying references from outgoing USD payment messages that involved countries, banks, or persons listed as parties or jurisdictions sanctioned by OFAC; (b) advising the countries, banks, and persons how to evade automated filters at U.S. financial institutions primarily located in New York, New York; and (c) causing U.S. financial institutions to process sanctioned transactions unknowingly.

810. Credit Suisse is a financial services company headquartered in Zurich, Switzerland. All of Credit Suisse's payment processing was handled in Switzerland and its Credit Suisse Asset Management Limited, United Kingdom ("CSAM") transactions were handled in London.

811. Credit Suisse's transactions were handled in London. "Credit Suisse is active in over 50 countries and has approximately 47,000 employees. The U.S. headquarters for Credit Suisse is located at 11 Madison Avenue, New York, New York. Credit Suisse serves clients worldwide through its Private Banking unit, which includes a Wealth Management and Corporate & Institutional Clients unit, an Investment Banking unit, and an Asset Management unit. Credit Suisse's New York branch is subject to oversight and regulation by the Board of Governors of the U.S. Federal Reserve System and the New York State Banking Department. The Swiss Financial Market Supervisory Authority (FINMA) is Credit Suisse's primary home-country regulator."<sup>45</sup>

---

<sup>45</sup> U.S. Dep't of Justice, *Exhibit A – Factual Statement*, <https://www.justice.gov/file/978881/download> (last visited Oct. 14, 2017).

812. From at least the mid-1990s to 2006, Credit Suisse used non-transparent methods to conduct USD transactions valued in the billions of USD on behalf of sanctioned entities, including Iran and Iranian entities.

813. Each such transfer was initiated by Defendant Credit Suisse and routed through a correspondent bank account in New York.

814. Such transfers substantively constitute a single course of conduct by Defendant Credit Suisse that entailed violations of U.S. laws in the same manner with respect to all Plaintiffs' claims. Additionally, this Court may exercise personal jurisdiction over Defendant Credit Suisse pursuant to Fed. R. Civ. P. 4(k)(1)(C), because Defendant Credit Suisse can be served in the United States pursuant to the ATA.

815. Defendant Credit Suisse resides, is found, or has an agent in the United States, specifically in the following states: Georgia; Michigan; Massachusetts; Illinois; Texas; California; Alabama; New York; Oregon; North Carolina; Washington, D.C.; Pennsylvania; and Florida.

**J. BANK SADERAT PLC**

816. In addition to the other banking defendants, Plaintiffs bring this case against Defendant Bank Saderat.

817. Bank Saderat Iran is one of the largest banks in Iran. It has approximately 3,400 offices worldwide, including, as discussed herein, a United Kingdom subsidiary (Defendant Bank Saderat).

818. Defendants sent or cleared USD payments through the U.S., including clearing done through U.S. subsidiaries.

819. Defendants maintained a correspondent bank accounts at financial institutions in New York and utilized the respective account to effectuate a significant number of wire transfers on behalf of Iran, its Agents and Proxies, and/or the Terrorist Groups.

820. In 2002, Bank Saderat Iran's London bank branch became a wholly-owned bank subsidiary, incorporated under United Kingdom law (*i.e.* Defendant Bank Saderat).

821. In October 2007, Defendant Bank Saderat, together with its parent company Bank Saderat Iran, was designated a SDGT by the United States pursuant to Executive Order ("E.O.") 13224.

822. The U.S. Treasury Department's 2007 press release regarding Bank Saderat's designation stated:

Bank Saderat, its branches, and subsidiaries: Bank Saderat, which has approximately 3200 branch offices, has been used by the Government of Iran to channel funds to terrorist organizations, including Hezbollah and European Union-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad. For example, from 2001 to 2006, Bank Saderat transferred \$50 million from the Central Bank of Iran through its subsidiary in London to its branch in Beirut for the benefit of Hezbollah fronts in Lebanon that support acts of violence.

823. Bank Saderat Iran was nationalized after the Iranian Revolution, but allegedly privatized in 2009. According to Bank Saderat Iran, 49% of its shares are owned by Iran, but it is technically a non-governmental entity.

824. Defendant Bank Saderat is the legal successor in interest to the Iran Overseas Investment Bank, London.

825. Iran Overseas Investment Bank changed its name to Bank Saderat Plc in March 2002.

826. Defendant Bank Saderat maintains its principal office in London, United Kingdom.

827. On July 1, 2005, OFAC determined that Bank Saderat Iran and its branches at 707 Wilshire Boulevard, Suite 4880, Los Angeles CA 90017 and at Lothbury, London EC2R 7HD, England are financial institutions owned or controlled by the Government of Iran within the meaning of 31 C.F.R. § 560.313.

828. On September 8, 2006, the United States Department of Treasury designated Bank Saderat as a SDGT, declaring that “Bank Saderat facilitates Iran’s transfer of hundreds of millions of dollars to Hizballah and other terrorist organizations each year. We will no longer allow a bank like Saderat to do business in the American financial system, even indirectly.”<sup>46</sup>

829. On October 25, 2007, the United States Department of Treasury, again designated Bank Saderat as a terrorist financier.

830. Bank Saderat Plc may be served in accordance with the Hague Convention by and through its registered office of Bank Saderat Plc, at 5 Lothbury, London, EC2R 7HD, England.

831. On March 3, 2008, The United Nations Security Council adopted Resolution 1803 (UNCSR 1803, 2008) by a vote of 14 in favor and none against, with 1 abstention (Indonesia), essentially black listing *all* banks domiciled in Iran, in particular Bank Saderat, and its branches and subsidiaries abroad.

832. On March 20, 2008, the U.S. Treasury Department’s Financial Crimes Enforcement Network (“FinCEN”) issued an advisory to supplement information previously provided on serious deficiencies present in the AML systems of the Islamic Republic of Iran. The Financial Action Task Force (“FATF”) had previously stated in October 2007 that Iran’s lack of a comprehensive anti-money laundering (“AML”) and combating the financing of

---

<sup>46</sup> See U.S. Dep’t. of Treasury, *Treasury Cuts Iran’s Bank Saderat off From U.S. Financial System* (Sept. 8, 2006) <https://www.treasury.gov/press-center/press-releases/Pages/hp87.aspx>.

terrorism regime represents a significant vulnerability in the international financial system. FinCEN further advised that, “through state-owned banks, the Government of Iran disguises its involvement in proliferation and terrorism activities through an array of deceptive practices specifically designed to evade detection. The Central Bank of Iran and Iranian commercial banks have requested their names be removed from global transactions in order to make it more difficult for intermediary financial institutions to determine the true parties in the transaction.”<sup>47</sup>

833. In March of 2010, the European Union also blacklisted Bank Saderat Iran and Saderat Plc. due to the banks’ provision of financial services related to Iran’s pursuit of nuclear weapons systems.

## VI. FACTUAL ALLEGATIONS

### A. ISLAMIC REPUBLIC OF IRAN A/K/A IRAN

834. Approximately 83 million people live in the country of Iran, which is approximately 2.5 times the size of Texas. Iran is located in the Middle East bordering seven countries including: Iraq, Afghanistan, Pakistan, Turkey, Armenia, Azerbaijan, and Turkmenistan.

#### 1. Iran Finances and Supports Terrorism and Terrorist Organizations

835. “Iran is designated as the world’s foremost state sponsor of terrorism and a direct threat to the national security of the United States and United States allies.”<sup>48</sup>

836. “Iran, through its ... (IRGC) ... provides material and financial support to [FTOs]...”<sup>49</sup>

---

<sup>47</sup> U.S. Dep’t of the Treasury, *Financial Crimes Enforcement Network*, [https://www.fincen.gov/statutes\\_regs/guidance/pdf/fin-2008-a002.pdf](https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2008-a002.pdf) (last visited Oct. 14, 2017).

<sup>48</sup> H.R. 566, 115<sup>th</sup> Cong. § 2(1) (2017); S. 420, 115<sup>th</sup> Cong. § 2(1) (2017).

<sup>49</sup> *Id.*

837. “Iran has systematically employed its national air carrier, Iran Air,<sup>50</sup> as well as numerous private and publically owned Iranian … air liners, including Mahan Air, to ferry weapons, troops, and military equipment on behalf of IRGC and Iran’s Ministry of Defense and Armed Forces Logistics (“MODAFL”) to FTOs and rogue regimes around the world.”<sup>51</sup>

838. “On June 23, 2011, the U.S. Department of Treasury designated Iran Air pursuant to Executive Order 13882 for providing material support and services to the IRGC, including shipping military-related equipment on behalf of the IRGC since 2006...”<sup>52</sup>

839. Iran has adopted a policy and practice of state-sponsored terrorism, including violent actions aimed directly at the United States, its allies, and its fundamental interests.

840. Elements of Iran’s Islamic Revolutionary Guard Corps (IRGC) were directly involved in the planning and support of terrorist acts throughout the region and continued to support a variety of groups in their use of terrorism to advance their common regional goals. Iran provided aid to Palestinian terrorist groups, Lebanese Hezbollah, Iraq-based militants, and Taliban fighters in Afghanistan.

841. The U.S. Department also stated in the report that Iran remains a threat to regional stability and U.S. interests in the Middle East because of its continued support for violent groups, such as HAMAS and Hezbollah.

842. The U.S. State Department concluded that Iranian authorities continued to provide lethal support, including weapons, training, funding, and guidance, to some Iraqi militant groups that target Coalition and Iraqi security forces and Iraqi civilians. The IRGC-QF, continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons,

---

<sup>50</sup> Iran Air remains owned and operated by the Iranian government.

<sup>51</sup> H.R. 566, 115<sup>th</sup> Cong. § 2(3) (2017); S. 420, 115<sup>th</sup> Cong. § 2(3) (2017).

<sup>52</sup> H.R. 566, 115<sup>th</sup> Cong. § 2(4) (2017); S. 420, 115<sup>th</sup> Cong. § 2(4) (2017).

mortars that have killed thousands of Coalition and Iraqi Forces, and EFPs that have a higher lethality rate than other types of improvised explosive devices (IEDs), and are specially designed to defeat armored vehicles used by Coalition Forces.

843. The IRGC-QF, in concert with Lebanese Hezbollah, provided training outside Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry. These individuals then passed on this training to additional militants inside Iraq, a “train-the-trainer” program.

844. The IRGC-QF and Hezbollah have also provided training inside Iraq. In fact, Coalition Forces captured a Lebanese Hezbollah operative in Iraq in 2007.

## **2. Economic Sanctions were Implemented to Stop Iran from Sponsoring Terrorism**

845. Before and throughout the Relevant Period, the U.S., the U.N., and the E.U., in a collective effort to stop Iran from sponsoring terrorism, implemented severe economic sanctions and enacted numerous laws, aimed at dramatically reducing Iran’s ability to receive proceeds from the sale of oil, Iran’s principal means of financial support.

846. The implemented economic sanctions were so severe that it was believed that Iran’s GDP would be cut in half, and therefore the sanctions would achieve their stated goal of forcing Iran to cease its financing of terrorism or face a revolt from within due to the catastrophic economic hardships that would face its citizens.

847. During the Relevant Period, Iran had the fourth largest oil reserves in the world. In 2005, the energy sector generated about 20% of Iran’s GDP, about 80% of its foreign exchange earnings, and about 50% of its government revenue. In short, Iran’s economic engine ran on oil.

848. To ensure that Iran was not able to profit from the export of oil - and therefore have funds available to fund terrorism - banks were prohibited from processing wire transfers to or from USD-denominated accounts owned or controlled by, individuals or companies, acting for or on behalf of Iran.<sup>53</sup>

849. Together these regulations strictly prohibited the type of US dollar clearing transactions that were being conducted by each Defendant on behalf of the Government of Iran, including the Central Bank of Iran, other Iranian financial institutions, and other individuals or companies, acting for or on behalf of the Government of Iran.

850. In addition, these regulations required Defendants to maintain accurate books, accounts, and records to reflect all transactions, including the type of USD clearing transactions, conducted by Defendants. In violation of the law, each Defendant falsified business records with the intent to defraud examiners and the intent to aid and assist sanctioned countries to engage in US dollar clearing transactions in violation of 31 C.F.R. 560.516.

851. In addition, these regulations demanded that Defendants follow strict reporting standards, and report the discovery of fraud, making of false entries, and omission of true entries, and other misconduct. In violation of the law, each Defendant engaged in elaborate schemes to conceal their illicit activities.

852. The economic sanctions specifically targeted USD-denominated wire transfers for several reasons. First, since the 1970s the USD has been the primary currency to buy and sell crude oil. Second, all three major crude benchmarks, Brent, WTI, and Dubai all price oil using

---

<sup>53</sup> Such laws include, but are not limited to 31 C.F.R. Parts 501, 535, 539, 544, 560-62, 566, 576, 590, and 594-98.

USD. Finally, Iran is a member of the Organization of Petroleum Exporting Countries (“OPEC”), and OPEC oil trades in U.S. dollars, commonly called petrodollars.

853. These regulations also made it illegal to structure transactions for the purpose of violating any of the prohibitions set forth in 31 C.F.R. Parts 560-598.

### **3. Need for the Conspiracy**

854. The economic sanctions were a major problem for Iran. If Iran was going to continue to sell its oil, while the sanctions were in place, Iran would need the assistance of large banks. Specifically, Iran needed the banks to intentionally disguise financial payments to and from USD-denominated accounts and conduct illicit trade-finance transactions on its behalf, to ensure that it could continue to sell its oil, grow its economy, and support terrorism.

855. Iran’s need for Defendants’ services was evident in emails obtained from SCB by the DFS in their decade long investigation of SCB’s USD clearing business.

856. In early 2001, Central Bank of Iran/Markazi approached SCB to act as its recipient bank for USD proceeds from daily oil sales made by the NIOC. SCB viewed this as “very prestigious” because “in essence, Standard Chartered Bank would be acting as Treasurer to the Central Bank of Iran...”<sup>54</sup>

857. Iran’s need to conspire is apparent in SCB’s December 10, 2012 Settlement Agreement with the U.S. Department of the Treasury. In the Factual Statement contained in the Settlement Agreement, SCB admits that Bank Markazi approached SCB in February 2001 about the possibility of opening an account to receive the proceeds of oil sales by the NIOC and certain additional Markazi funds. The factual statement outlines how SCB and Markazi began to

---

<sup>54</sup> Email from Standard Chartered Bank’s Head of Inbound Sales, Institutional Banking, to Standard Chartered Bank’s Head of Group Market Risk, and Standard Chartered Bank’s Group Head of Institutional Banking and Global Head of Business Segment, and its Head of Funds Management dated February 19, 2001, SCB INT 0005352.

develop operating procedures to mask the involvement of Iranian entities in payment instructions sent to SCB's New York Branch.

**4. Who Best to Conspire With**

858. To Defendants, Iran represented a source of fee income, as limitless as Iran's supply of oil, well worth the risk of breaking the law. The defendant banks were well aware of both the risks and rewards of doing business with State Sponsors of Terrorism.

**5. Defendants Were Warned Not To, But They Did It Anyway**

859. In April 2003, with 9/11 still fresh in the minds of American regulators, the Federal Reserve sent HSBC's American subsidiary a cease-and-desist letter, ordering it to clean up its act and make a better effort to keep criminals and terrorists from opening accounts at its bank.

860. In March 2004, the Federal Reserve sent Crédit Agricole S.A., Crédit Agricole Indosuez, and Credit Lyonnais S.A. a cease-and-desist letter and to take specific steps to enhance and improve their internal controls, risk management, compliance, audit, and regulatory reporting functions.

861. In October 2004, the Federal Reserve sent Standard Chartered plc, Standard Chartered Bank, and Standard Charter a cease-and-desist letter, ordering it to make a better effort to improve their AML procedures and policies, and specifically to no longer allow correspondent accounts for foreign shell banks.

862. In October 2005, the Federal Reserve sent Deutsche Bank Trust Company Americas a cease-and-desist letter, ordering it to also clean up its act and make a better effort to improve their AML procedures and policies, and to comply with the Currency and Foreign Transaction Reporting Act. During the Relevant Period, Defendants knew that Iran had been

designated as a State Sponsor of Terrorism since 1984, and linked to many terrorist organizations and incidents around the world.

863. Defendants also knew that sanctions were imposed against Iran with the sole and specific purpose of stopping Iran's sponsorship of terrorism, and that in order for the sanctions to work they must prevent Iran from selling oil. If Iran was not prevented from selling oil, Iran would have no reason to stop sponsoring terrorism. Despite having this knowledge, Defendants deliberately conspired with Iran to sell billions of dollars' worth of oil, in violation of the sanctions.

864. Defendants knew the economic sanctions were put in place to cripple the Iranian economy, which would force Iran's leaders to cease their sponsorship of terrorism, which could after a period of time result in the sanctions being lifted. Despite having knowledge of the purpose of the sanctions, the banks processed billions of USD in wire transfers for the benefit of Iran in direct violation of the sanctions.

## **6. Effect of Defendants' actions on Iran's Economy**

865. As a result of the sheer size and scale of operations, collectively Defendants were able to not only overcome the sanctions imposed by the U.S., the U.N., and the E.U. on Iran, but they enabled Iran to dramatically expand its economy during the 8 year period the sanctions were in place.

866. Defendants' participation in the Conspiracy was substantial for several reasons. First, Defendants collectively transferred via wire, hundreds of billions of dollars during the course of the Conspiracy. Second, Defendants acted as "facilitators" rather than just providing "criminal assistance." Third, Defendants provided trade financing, effectively mitigating the risks associated with selling oil on the black market.

867. As a direct result of Defendants' actions, Iran benefited from the illegal sale of its oil on the world market, and filled its coffers with funds that were now available to fund its illicit campaign of terror.

868. Also as a result of Defendants' actions, Iran was also able to freely transfer money earned from its illegal oil sales, to purchase items prohibited under the sanctions.

869. As a result of the billions of USDs Defendants transferred on behalf of Iran, the sanctions did not have any detrimental effect on Iran's economy. Defendants' acts were substantial, not only in terms of total dollars, but the effect that it had on Iran's Exports, GDP, and ultimately Iran's need and desire to stop sponsoring terrorism.

870. Iran committed and continues to commit violent attacks against the U.S. nationals. Iran commits these attacks via proxy terrorist organizations made up of Iranian, Lebanese, Iraqi, Afghani, and Yemeni citizens and citizens of other countries.

871. According to the CIA, Iranian leaders view terrorism as an important instrument of foreign policy used both to advance national goals and to export the regime's Islamic revolutionary ideals.<sup>55</sup>

872. Further, Iran supports and sometimes directs terrorist operations by Hezbollah and it is the desire of the Iranian leaders to keep the United States as a primary terrorist target.<sup>56</sup>

873. In June 2007, U.S. Department of State spokesman, Sean McCormack, delivered a press briefing on Iran and its ties to international terrorism. When asked what changes he was looking for concerning Iran and its ties to terrorism, he responded, “[w]ell, for starters, stop

---

<sup>55</sup> Central Intelligence Agency, Directorate of Intelligence, *Iran: The Uses of Terror* (Oct. 22, 1987), [https://www.cia.gov/library/readingroom/docs/DOC\\_0000259360.pdf](https://www.cia.gov/library/readingroom/docs/DOC_0000259360.pdf).

<sup>56</sup> *Id.*

supplying *money, technology, and training* for people who are trying to kill [U.S. nationals]....”]...”<sup>57</sup> (Emphasis added).

#### **7. Iran’s Long History of Materially Supporting And Encouraging Acts of International Terrorism**

874. For decades, Iran has made the funding of terrorist organizations (including the Special Groups and other terrorists that perpetrated the Terrorist Attacks) and the commodification of international acts of terrorism its business.

875. Iran has a history of financing, supporting, and training terrorists and their affiliates in the perpetration of terrorist attacks against the United States, its citizens, and its allies. For example, the Honorable John D. Bates held in a lawsuit brought by U.S. victims of the bombing of the U.S. embassies in Nairobi and Dar es Salaam that, “[s]upport from Iran and Hezbollah was critical to al Qaeda’s execution of the 1998 embassy bombings.... . . . Prior to its meetings with Iranian officials and agents, al Qaeda did not possess the technical expertise required to carry out the embassy bombings.”<sup>58</sup>

876. Iran’s support for these groups is expansive. By 2009, Israeli intelligence estimated that Iran had provided over \$1 billion in direct support to Hezbollah.<sup>59</sup>

877. Iran has been lavish with its support to all groups (including Sunni groups with ties to al Qaeda) engaged in acts of international terrorism against Iraqi citizens, Coalition Forces, and U.S. nationals, including Plaintiffs.

---

<sup>57</sup> U.S. Dep’t of State, *Daily Press Briefing by Department Spokesman Sean McCormack* (June 27, 2007), <http://site-894736.bcvp0rtal.com/detail/videos/archive/video/1807599216/daily-briefing---june-27-2007>.

<sup>58</sup> Memorandum Opinion at 13–14, *Wamai v. Republic of Sudan et. al.*, No. 1:08-cv-01349-JDB-JMF (D.D.C. Nov. 30, 2011), ECF No. 55.

<sup>59</sup> U.S. Senate on Foreign Relations Subcommittee on Near Eastern and Central Asian Affairs, *Testimony of Dr. Matthew Levitt, Director, Stein Program on Counterterrorism and Intelligence, The Washington Institute for Near East Policy, Iran’s Support for Terrorism in the Middle East* (Jul. 25, 2012), [https://www.foreign.senate.gov/imo/media/doc/REVISED\\_Matthew\\_Levitt\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/REVISED_Matthew_Levitt_Testimony.pdf).

878. Iran provided material support and resources for the commission of acts of extrajudicial killing, torture, and/or hostage taking within the meaning of 28 U.S.C. § 1605A, including the Terrorist Attacks in which Plaintiffs were killed, injured, or maimed, and performed actions that caused the Terrorist Attacks and the harm to Plaintiffs herein.

879. The Government of Iran is politically and ideologically hostile to the United States and its allies, and has consistently provided material support for acts of international terrorism, including extrajudicial killings, torture, and hostage takings, particularly through the IRGC, the IRGC-QF, and the Lebanese-based FTO, Hezbollah, which historically has served as Iran's proxy and agent, enabling Iran to project extremist violence and terror throughout the Middle East and around the globe.

880. Since the Iranian Revolution in 1979, Iran has been a principal source of extremism and terrorism throughout the Middle East and the rest of the world.

881. Iran acts through co-conspirators and/or agents and offers bounties for killing U.S. nationals, shooting down U.S. helicopters, and destroying American tanks. Reports suggest that in fall 2003 "a senior Iranian cleric in Tehran set up a special 100-member army, known as al Saqar, which means eagle in Arabic, to . . . carry out [acts of international terrorism]."<sup>60</sup>

882. In Iraq, the policies of Iran have been largely successful, "giving Iran an unprecedented degree of influence there at the expense of the United States...." An Iran-friendly Iraq "serves as an opportunity for Iran to evade the increasingly harsh international sanctions regime and to continue financing [FTOs]."<sup>61</sup>

---

<sup>60</sup> Edward T. Pound, *Special Report: The Iran Connection*, U.S. News and World Report, Nov. 14, 2004.

<sup>61</sup> Frederick W. Kagan *et al.*, *Iranian Influence in the Levant, Egypt, Iraq, and Afghanistan*, at 6 (May 2012), [http://www.aei.org/wp-content/uploads/2012/05/-iranian-influence-in-the-levant-egypt-iraq-and-afghanistan\\_171235465754.pdf](http://www.aei.org/wp-content/uploads/2012/05/-iranian-influence-in-the-levant-egypt-iraq-and-afghanistan_171235465754.pdf).

883. Unclassified Iraqi government Harmony records, collated by the Combating Terrorism Center at West Point, as well as information provided to the Coalition Forces through interrogation of detainees of the Shia militias, illustrate how Iran sponsored terrorist groups, directly and through Hezbollah (Iran's proxy for more than 30 years), operated in Iraq, including supporting and directing the terrorist groups responsible for the Terrorist Attacks which killed or injured Plaintiffs or their family members.<sup>62</sup>

884. Planning and preparation by Iran and its Agents and Proxies, including Hezbollah, for their active involvement in supporting terrorist groups and encouraging sectarian violence in Iraq has been underway since at least 2002.

885. At least as early as the 2003 U.S. overthrow of Saddam Hussein's regime in Iraq, Iran has assiduously worked to expand its influence in Iraq and throughout the region in a variety of ways, including by fomenting violence and terrorism when such activities have served its diplomatic, political, and economic ambitions.

886. When Coalition Forces liberated Iraq in 2003, the IRGC formed the counter-Coalition Ramazan Corps and ordered it to attack U.S. and Iraqi forces. Saddam Hussein's 24-year rule ended on April 9, 2003. The U.S. Department of State reported that, shortly thereafter, individuals with ties to the IRGC may have attempted to infiltrate southern Iraq, and elements of the Iranian regime helped members of AAI (previously and subsequently known by several different names, including Ansar Al-Sunnah) transit and find safe haven in Iran. In a Friday prayers sermon in Tehran in May 2003, secretary general of Iran's powerful Guardian Council Ayatollah Ahmad Jannati publicly encouraged Iraqis to stage and participate in suicide

---

<sup>62</sup> Joseph Felter and Brian Fishman, *Iranian Strategy in Iraq: Politics and 'Other Means,'* Combating Terrorism Center, West Point, 2008. See Appx. B, which contains Ba`ath-era intelligence documents.

operations against U.S. nationals, including Plaintiffs, and Coalition Forces.<sup>63</sup> He went on to encourage the so-called “holy fighters” to “conduct attacks against American troops.”<sup>64</sup>

887. In 2005, the Department of State reported that Iran was a safe haven in that known terrorists, extremists, and sympathizers are able to transit its territory and cross the long and porous border into Iraq. Iran also equips terrorists with technology and provides training in extremist ideology and militant techniques.<sup>65</sup>

888. In 2008, William Burns, U.S. Undersecretary of State for Political Affairs, testified before Congress that it is “Iran’s... support for terrorist groups...its efforts to sow violence and undermine stability in Iraq and Afghanistan, including lethal support for groups that are directly responsible for hundreds of U.S. casualties.”<sup>66</sup>

889. As recently as 2015, the State Department stated that “Iran’s state sponsorship of terrorism worldwide remained undiminished through the ... IRGC-QF, its Ministry of Intelligence and Security, and Tehran’s ally Hezbollah, which remained a significant threat to the stability of Lebanon and the broader region.”<sup>67</sup>

---

<sup>63</sup> U.S. Dep’t of State, Office of the Coordinator for Counterterrorism, *Patterns of Global Terrorism* (Apr. 29, 2004), <http://www.state.gov/j/ct/rls/crt/2003/31644.htm>.

<sup>64</sup> Pound, *supra* note60.

<sup>65</sup> U.S. Dep’t of State, Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2005*, 21 (Apr. 2006), <https://www.state.gov/documents/organization/65462.pdf>.

<sup>66</sup> U.S. Dep’t of State, *Testimony by William J. Burns, Undersecretary for Political Affairs: U.S. Policy Towards Iran: Hearing Before S. Comm. on Foreign Relations and H. Comm. on Foreign Affairs* (July 9, 2008).

<sup>67</sup> U.S. Dep’t of State, Office of the Coordinator for Counterterrorism, *Country Reports on Terrorism 2015*, 166 (June 2016), <https://www.state.gov/documents/organization/258249.pdf>.

## 8. Iran's Sponsorship and Material Support of Terrorism in Iraq

890. Operating “through proxies and trusted operatives, is Iran’s trademark modus operandi.”<sup>68</sup>

891. Iran utilizes Special Groups and other terrorists that coordinated with Hezbollah and the IRGC, as front groups to perpetrate terrorist acts, including those that killed or injured Plaintiffs or members of Plaintiffs’ families.

892. Iran’s support of terrorist groups in Iraq was described in the U.S. State Department’s 2005 Country Reports on Terrorism, which observed:

Iran has provided political and ideological support for several terrorist and militant groups active in Iraq. Attractive to terrorists in part because of the limited presence of the United States and other Western governments there, Iran is also a safe haven in that known terrorists, extremists, and sympathizers are able to transit its territory and cross the long and porous border into Iraq. Iran also equips terrorists with technology and provides training in extremist ideology and militant techniques.

893. Iran furthers its terrorism-based foreign policy through the following key Iranian Agents and Proxies: MODAFL, the IRGC, the IRGC-QF, Hezbollah/Hizbullah, and Special Groups.

894. In 2008, Pentagon Press Secretary Geoff Morrell reported on the “smuggling system in which the Iranians are providing their allies within Iraq, these special groups, with the munitions that are then used to take on us, whether it be EFPs or rockets or conventional arms. These are being used by these special groups and being provided by the Iranians.”

895. On January 9, 2008, the U.S. Treasury Department designated certain individuals under E.O. 13438 for threatening the peace and stability of Iraq and the government of Iraq,

---

<sup>68</sup> U.S. Senate on Foreign Relations Subcommittee on Near Eastern and Central Asian Affairs, *Testimony of Dr. Matthew Levitt, Director, Stein Program on Counterterrorism and Intelligence, The Washington Institute for Near East Policy, Iran’s Support for Terrorism in the Middle East* (July 25, 2012), [https://www.foreign.senate.gov/imo/media/doc/REVISED\\_Matthew\\_Levitt\\_Testimony.pdf](https://www.foreign.senate.gov/imo/media/doc/REVISED_Matthew_Levitt_Testimony.pdf).

including Ahmed Foruzandeh (a Brigadier General in the IRGC-QF), Abu Mustafa Al-Sheibani, and Isma'il Hafiz Al Lami (a/k/a “Abu Dura”), all of whom were based in Iran and/or received funding from Iran.

896. Regarding the designation of Abu Mustafa Al-Sheibani, the Treasury Department press release stated:

Iran-based Abu Mustafa Al-Sheibani leads a network of Shia extremists that commit and provide logistical and material support for acts of violence that threaten the peace and stability of Iraq and the Government of Iraq. Al-Sheibani’s Iran-sponsored network was created to affect the Iraqi political process in Iran’s favor. The network’s first objective is to fight U.S. forces, attacking convoys and killing soldiers. Its second objective is to eliminate Iraqi politicians opposed to Iran’s influence. *Elements of the IRGC were also sending funds and weapons to Al-Sheibani’s network.*

Al-Sheibani’s network – consisting of several hundred members – conducted IED attacks against Americans in the Baghdad region. As of March 2007, Al-Sheibani, known to transport Katyusha rockets to be used for attacks against Coalition Forces, launched rockets against Americans and made videos of the attacks to get money from Iran. *As of April 2007, a member of Al-Sheibani’s network supervised the transport of money and explosives from Iran for eventual arrival in Baghdad.* In early May 2007, Al-Sheibani’s network assisted members of a Shia militia group by transporting them to Iran for training and providing them with weapons for their activities in Iraq.

Additionally, Al-Sheibani commands several pro-Iranian insurgent groups in southern Iraq that work to destabilize Iraq and sabotage Coalition efforts. These groups use a variety of weapons, to include mortars, Katyusha rockets, and anti-tank landmines. *Ordered by IRGC headquarters to create disorder, the task of these groups is to attack bases of Coalition Forces in southern Iraq, particularly British forces.*

(Emphasis added).

897. Iran’s objectives were not secret. Its pursuit and development of weapons of mass destruction (“WMDs”)—including IEDs, EFPs, mines, and similar explosive munitions — were the subject of hundreds of news reports, U.S. government reports, and Congressional testimony, as well as U.N. Security Council resolutions and European Union regulations.

898. According to a 2010 report by the Combating Terrorism Center at West Point, Iran paid Iraqi “insurgent” groups “between \$4,000 and \$13,000 per rocket or roadside bomb.”

899. As former Central Intelligence Director and National Security Agency Director Air Force General Michael V. Hayden explained in the book *American Intelligence in the Age of Terror – Playing to the Edge*, 292–93 (2016), Iran and its Agents and Proxies sponsored and committed terrorist acts in Iraq against United States citizens:

This is about deterring us. Look at their behavior – with Hamas, with Hezbollah, in Iraq, in Afghanistan. Hell, we judge that it is the policy of the Iranian government – approved at the highest levels of that government – to facilitate the killing of young Americans and other allies in Iraq...

Iran was already an incredibly destabilizing force in the region, especially in Iraq. The Badr Corps, of the most important Shia militias in Iraq, was an arm of Iranian policy. Tehran also had enlisted the aid of its Lebanese proxy Hezbollah and its murderous operations chief, Imad Mughniyah, to create a Hezbollah clone in Iraq, an effort supported by several training camps in Iran.

The [IRGC-QF] was also aggressive on the ground. It helped plan a deadly raid – complete with faked identity cards and American-style uniforms against a U.S. checkpoint near Karbala in January 2007 that resulted in five soldiers killed (four of whom had been kidnapped). The [IRGC-QF] was also manufacturing and shipping EFPs-explosively formed projectiles-to Shia militias. These were ingeniously designed shaped-charged devices that could penetrate even the thickest American armor. EFPs were the biggest killers of Americans in Iraq, and we knew, with high confidence, that this was the Iranian government’s intent.

And they weren’t bashful about any of this. Soleimani famously sent a text message to Iraqi president Talabani for the US commander: “General Petraeus, you should know that I, Qassem Soleimani, control policy for Iran with respect to Iraq, Lebanon, Gaza, and Afghanistan. The ambassador in Baghdad is a [IRGC-QF] member. The individual who’s going to replace him is a [IRGC-QF] member.

## **9. Islamic Revolutionary Guard Corps**

900. The IRGC was founded in the wake of the 1979 revolution as a branch of the Iranian Armed Forces tasked with protecting the country’s Islamic system. Since its origin as an ideologically driven militia, the IRGC has taken an ever more assertive role in virtually every aspect of Iranian society. The IRGC is a special entity unto itself, part military force, part

paramilitary force, and part business conglomerate.<sup>69</sup> Its expanded social, political, military, and economic role has led many analysts to argue that its political power has surpassed even that of the Shia clerical system.<sup>70</sup>

901. The IRGC nominally comprises five branches (Ground Forces, Air Force, Navy, Basij militia, and the IRGC-QF special operations IRGC-QF) in addition to a counter-intelligence directorate and representatives of the Supreme Leader.

902. According to the U.S. State Department's 2005 Country Reports on Terrorism: “[t]he IRGC was increasingly involved in *supplying lethal assistance* to Iraqi militant groups, which destabilizes Iraq ... Senior Iraqi officials have publicly expressed concern over Iranian interference in Iraq, and there were reports that *Iran provided funding, safe passage, and arms to insurgent elements.*” (Emphasis added).

903. The IRGC is the spine of the current political structure and a major player in the Iranian economy.<sup>71</sup> It has expanded well beyond its mandate into a socio-military-political-economic force that deeply penetrates Iran's power structure.<sup>72</sup> The IRGC is a central participant in the Conspiracy.

904. The IRGC has also infiltrated Iraqi society, providing “political and ideological support” via charitable associations such as the Khomeini Social Help Committee – in Karbala, Najaf, Kut, and Sadr City – and the Imam Mohammad Bagher Institute in Najaf.

---

<sup>69</sup> Robert Baer, THE DEVIL WE KNOW: DEALING WITH THE NEW IRANIAN SUPERPOWER 127 (2008).

<sup>70</sup> Geneive Abdo, *The Rise of the Iranian Dictatorship*, FOREIGN POLICY MAGAZINE Oct. 7, 2009.

<sup>71</sup> Mehdi Khalaji, *The Washington Institute for Near East Policy (Policy #1273) Iran's Revolutionary Guards Corps, Inc.* (Aug. 17, 2007), <http://www.washingtoninstitute.org/policy-analysis/view/irans-revolutionary-guards-corps-inc>.

<sup>72</sup> Council on Foreign Relations, *Iran's Revolutionary Guards* (Oct. 12, 2011), <https://www.cfr.org/backgrounder/irans-revolutionary-guards>.

905. The IRGC also purchased or developed seven television stations in Iraq, and at least three radio stations.

906. All of these “investments” required substantial funding in USD funds (as Iraqi local currency was not widely accepted in Iraq during this time period).

#### **10. Islamic Revolutionary Guard Corps-Qods Force**

907. The highest echelons of the Iranian government and of Hezbollah have worked together to organize a violent, Shia resistance movement in Iraq. The IRGC-QF, with direct assistance from Iran, has established and funded this movement.

908. The IRGC-QF is the IRGC unit tasked with extraterritorial operations. It trains and equips Islamic revolutionary groups around the Middle East. The IRGC-QF typically provides this paramilitary instruction in Iran. At times, the IRGC-QF plays a more direct role in the military operations of the forces it trains, including pre-attack planning and other operation-specific strategic advice.

909. The IRGC-QF’s “Department 2000” manages Iran’s relationship with Hezbollah, which includes the flow of some of Iran’s most sophisticated weapon systems, including military grade EFPs, anti-tank guided missiles, and various rockets, such as the Fajr-5.

910. Since 2003, Iran has been materially supporting acts of international terrorism by advising, organizing, training, funding, and equipping FTOs, Special Groups, AAI, and other terrorists to kill, maim, or otherwise injure U.S. nationals, among others. To do this, Iran enlisted (and continues to enlist) the IRGC-QF to provide such support to these FTOs and Special Groups.

911. In October 2007, the United States designated the IRGC-QF a SDGT pursuant to E.O. 13324, explaining that:

The Qods Force has had a long history of supporting Hizballah’s military,

paramilitary, and terrorist activities, providing it with guidance, funding, weapons, intelligence, and logistical support. The Qods Force operates training camps for Hezbollah in Lebanon's Bekaa Valley and has reportedly trained more than 3,000 Hezbollah fighters at IRGC training facilities in Iran. The Qods Force provides roughly \$100 to \$200 million in funding a year to Hezbollah and has assisted Hezbollah in rearming in violation of UN Security Council Resolution 1701.

*In addition, the Qods Force provides lethal support in the form of weapons, training, funding, and guidance to select groups of Iraqi Shi'a militants who target and kill Coalition and Iraqi forces and innocent Iraqi civilians.*

(Emphasis added).

912. In 2004, the IRGC-QF began flooding Iraq with EFPs. These EFPs wreaked havoc on American troops. EFPs require skilled assembly and rely on sophisticated sensors. According to General Stanley McChrystal, then head of Joint Special Operations Command, “[t]here was zero question where [the EFPs] were coming from. We knew where all the factories were in Iran. The EFPs killed hundreds of Americans.”<sup>73</sup>

913. On October 25, 2007, when the U.S. Department of Treasury designated IRGC-QF as SDGT under E.O. 13224, the Department cited the IRGC-QF’s material support to the Taliban, Lebanese Hezbollah, Hamas, Palestinian Islamic Jihad, and the Popular Front for the Liberation of Palestine-General Command as evidence of Iran seeking to inflict casualties on U.S. and NATO forces.<sup>74</sup>

914. IRGC-QF controls and commands Hezbollah. Pursuant to instructions from IRGC-QF, Hezbollah formed Unit 3800. Unit 3800 was tasked by the IRGC-QF with recruiting,

---

<sup>73</sup> Dexter Filkins, *The Shadow Commander*, THE NEW YORKER, Sept. 30, 2013, <http://www.newyorker.com/magazine/2013/09/30/the-shadow-commander>.

<sup>74</sup> U.S. Dep’t of the Treasury, *Fact Sheet: Designation of Iranian Entities and Individuals for Proliferation Activities and Support for Terrorism* (Oct. 25, 2007), <https://www.treasury.gov/press-center/press-releases/Pages/hp644.aspx>.

radicalizing, and training Iraqi militants and organizing several Iraqi terrorist/insurgency militias, called Special Groups.

915. According to Brigadier Gen. Kevin J. Bergner, a U.S. military spokesman who previously served as the Deputy Commanding General for MNF-I in Mosul, Iraq, “the Qods Force has provided armor-piercing weapons to extremist groups in Iraq, funneling them up to \$3 million a month and training Iraqi militiamen at three camps near Tehran.” General Bergner added, “[t]he Iranian Qods Force is using Lebanese Hezbollah essentially as a proxy, as a surrogate in Iraq.”

## **11. Hezbollah**

916. Iran has had a long, deep, strategic partnership with the Lebanese-based FTO Hezbollah, which historically has served as Iran’s proxy and agent, enabling Iran to project extremist violence and terror throughout the Middle East and around the globe.

917. Hezbollah is probably the most prominent group developed with the assistance of the IRGC-QF.

918. In a televised speech in June 2016, the leader of Hezbollah, Sheikh Hassan Nasrallah, claimed that “We are open about the fact Hezbollah’s budget, its income, its expenses, everything it eats and drinks, its weapons and rockets, come from the Islamic Republic of Iran.” Nasrallah stated that, “[a]s long as Iran has money, we have money... Just as we receive the rockets that we use to threaten Israel, we are receiving our money. No law will prevent us from receiving it....”<sup>75</sup>

919. Hezbollah’s forces are trained and organized by a contingent of 1,500

---

<sup>75</sup> Majid Rafizadeh, *In first, Hezbollah confirms all financial support comes from Iran*, AL ARABIYA ENGLISH (Jun. 25, 2016), <https://english.alarabiya.net/en/2016/06/25/In-first-Hezbollah-s-Nasrallah-confirms-all-financial-support-comes-from-Iran.html>.

Revolutionary Guards. Hezbollah's strength has grown so significantly that its paramilitary wing, the Jihad Council, is considered more powerful than the Lebanese Army. Hezbollah relied almost exclusively on Iranian largesse, which funds at least \$100 to \$200 million a year or more.<sup>76</sup>

920. The Iranian regime provides "extensive financial support for terrorists generally and in support for al Qaeda and Hezbollah in particular."<sup>77</sup>

921. Iran "created Hizballah...[and] has been the sponsor of Hizballah since its inception, providing funding, training, leadership, and advice via Hizballah's leadership councils...Hizballah has received from Iran \$100 million to \$500 million in direct financial support annually...Hizballah served as a terrorist proxy for Iran, created specifically for the purpose of serving as a front for Iranian terrorism, in effect, a cover name for terrorist operations run by Iran's IRGC around the world."<sup>78</sup>

922. On January 25, 1995, Hezbollah was designated a SDT by the United States.

923. Hezbollah was designated an FTO by the United States on October 8, 1997.

924. On October 31, 2001, pursuant to E.O. 13224, Hezbollah was designated SDGT by the United States.

925. As the U.S. government noted when it designated Defendant Bank Saderat a SDGT, Defendant Bank Saderat has provided at least \$50 million to Hezbollah.

926. Sometime after the 2003 U.S. invasion of Iraq, at Iran's request Hezbollah leader

---

<sup>76</sup> U.S. Dep't of Defense, *CDA—Military Power of Iran, Unclassified Report on Military Power of Iran* (Apr. 2010), [http://www.fas.org/man/eprint/dod\\_iran\\_2010.pdf](http://www.fas.org/man/eprint/dod_iran_2010.pdf).

<sup>77</sup> See, e.g., *Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 135–36 (D.D.C. 2011); *Kaplan v. Cent. Bank of the Islamic Republic of Iran*, 55 F. Supp. 3d 189, 197 (D.D.C. 2014).

<sup>78</sup> STEVEN R. WARD, IMMORTAL: A MILITARY HISTORY OF IRAN AND ITS ARMED FORCES 320 (2009).

Hassan Nasrallah created “Unit 3800,” an entity dedicated to supporting Iraqi Shi'a terrorist groups targeting Iraqi citizens, and MNF-I.

927. Unit 3800 has trained and advised various Shi'a militias in Iraq, later termed the Special Groups.

928. By early 2005, the presence of Hezbollah operatives in Iraq became an open secret when Iraqi Interior Minister Falah al-Naqib announced the arrest of eighteen Hezbollah members on terrorism charges.

929. According to U.S. intelligence estimates—and following the 2007 arrest and interrogation of Hezbollah's senior operative in Iraq—in 2007 the IRGC-QF provided Hezbollah and one of its local trainers, Ali Musa Daqduq (who is discussed in greater detail below), up to \$3,000,000.00 in U.S. currency *every month*.

930. United States District Courts have found in numerous lawsuits related to international acts of terrorism sponsored or directed by Iran that Hezbollah is, in fact, an arm of the IRGC and a key component to Iran's *modus operandi* of sponsoring and/or directing international terrorism aimed primarily against the United States and its allies.<sup>79</sup>

## **12. Iran's Ministry of Defense and Armed Forces Logistics**

931. In October 2007, the United States designated MODAFL, stating it controls the Defense Industries Organization (“DIO”), an Iranian entity identified in the Annex to UN Security Council Resolution 1737 and designated by the United States under E.O. 13382 on March 30, 2007.

932. MODAFL is the principal procurement branch of Iran's military/terror apparatus.

---

<sup>79</sup> See, e.g., *Owens v. Republic of Sudan*, 826 F. Supp. 2d 128, 135–36 (D.D.C. 2011); *Kaplan v. Cent. Bank of the Islamic Republic of Iran*, 55 F. Supp. 3d 189, 197 (D.D.C. 2014).

933. MODAFL operates the [Iran] Aviation Industries Organization, the Aerospace Industries Organization (“AIO”), and the DIO. MODAFL was designated by the United States on October 25, 2007.

934. The AIO was designated under E.O. 13382 on June 28, 2005 for weapons proliferation.

935. The MAPNA group is also a key component of MODAFL and the IRGC’s procurement chain.

936. Abbas Aliaabadi, Chairman of MAPNA International FZE and President of the MAPNA Group, is a former member of the Iranian Ministry of Construction Jihad and of the Iranian Air Force. Aliaabadi was also a key member of the Ministry of Culture & Islamic Guidance instrumental in the creation of Hezbollah and has close links to the IRGC.

937. Pursuant to the Arms Export Control Act and the Export Administration Act, MODAFL was sanctioned in November 2000 for its involvement in missile technology proliferation activities.

938. The U.S. government explained the basis for the designation as follows:

The Ministry of Defense and Armed Forces Logistics (MODAFL) controls the Defense Industries Organization, an Iranian entity identified in the Annex to UN Security Council Resolution 1737 and designated by the United States under E.O. 13382 on March 30, 2007. MODAFL also was sanctioned, pursuant to the Arms Export Control Act and the Export Administration Act, in November 2000 for its involvement in missile technology proliferation activities.

MODAFL has ultimate authority over Iran’s Aerospace Industries Organization (AIO), which was designated under E.O. 13382 on June 28, 2005. The AIO is the Iranian organization responsible for ballistic missile research, development and production activities and organizations, including the Shahid Hemmat Industries Group and the Shahid Bakeri Industries Group, which were both listed under UN Security Council Resolution 1737 and designated under E.O. 13382. The head of MODAFL has publicly indicated Iran’s willingness to continue to work on ballistic missiles. Defense Minister Brigadier General Mostafa Mohammad Najjar said that one of MODAFL’s major projects is the manufacturing of Shahab-3 missiles and that it will not be halted. MODAFL representatives have acted as

facilitators for Iranian assistance to an E.O. 13382-designated entity and, over the past two years, have brokered a number of transactions involving materials and technologies with ballistic missile applications.

939. Formally, the IRGC is a subordinate directorate of MODAFL.

940. The IRGC uses MODAFL to both procure and develop weapons and equipment for its use.

941. The DIO, the AIO, and Defense Technology and Science Research Centre are all subordinate to MODAFL, giving it operational control over Iran's ballistic missile development program.<sup>80</sup>

942. MODAFL entities' illicit procurement activities have resulted in a series of ongoing U.S. sanctions.<sup>81</sup>

943. The Special Groups to which Iran provides material resources and support include but are not limited to multiple Shia (and some Sunni) terror groups in Iraq, including, KH, AAH, JAM, the Badr Organization; and the Taliban. Hamas, Lebanese Hezbollah, and the Palestinian Islamic Jihad maintain representative offices in Tehran in part to help coordinate Iranian financing and training.

### **13. The Iranian Ministry of Intelligence and Security**

944. The Iranian Ministry of Intelligence and Security (a/k/a "Vezarat-e Ettela'at Va Amniyat-e Keshvar" a/k/a "VEVAK" a/k/a "VAJA," hereinafter "MOIS") is located in Tehran.

945. MOIS is the most powerful and well-supported ministry among all Iranian ministries in terms of logistics, finances, and political support. It is a non-military governmental organization that operates both inside and outside of Iran.

---

<sup>80</sup> STEVEN R. WARD, *Immortal: A Military History of Iran and Its Armed Forces* 320 (2009).

<sup>81</sup> In November 2000, the United States sanctioned MODAFL pursuant to the Arms Export Control Act, the Export Administration Act; and, also in October 2007, in accordance with Exec. Order No. 13382 (June 25, 2005).

946. MOIS functions as the Iranian Intelligence Service and, in this capacity, it is the secret police and primary intelligence agency of the Islamic Republic of Iran. It is the part of the Iranian government's security apparatus responsible for the assassination of Iranian political dissidents inside and outside the country.

947. MOIS uses all means at its disposal to protect the Islamic Revolution of Iran, utilizing such methods as infiltrating internal opposition groups, monitoring domestic threats and expatriate dissent, arresting alleged spies and dissidents, exposing conspiracies deemed threatening, and maintaining liaison with other foreign intelligence agencies as well as with organizations that protect the Islamic Republic's interests around the world.

948. MOIS operates under the direct supervision of Iran's Supreme Leader, Ayatollah Khamenei, who claims to be the leader of the Muslim world. As noted above, MOIS agents are known as "Unknown Soldiers of Imam Zaman," who is the Twelfth Imam in the succession of Islamic leaders of Shi'a Muslims. However, the organization is not bound by Shi'a beliefs. To advance its goals, MOIS recruits individuals regardless of their beliefs.

949. According to Iran's constitution, all organizations must share information with the Ministry of Intelligence and Security. The ministry oversees all covert operations. The IRGC and IRGC-QF Qods Force share all the information they collect with MOIS.

950. MOIS and the IRGC-QF coordinate through foreign embassies, "charities," and cultural centers in targeted countries.

951. Hezbollah is organizationally linked to MOIS, and is used by MOIS as a proxy in Iran's intelligence operations.

952. In the Middle East, Iran, through MOIS and the IRGC-QF, uses Hezbollah to threaten the United States in Iraq and Afghanistan by backing insurgent groups, including Terrorist Groups who committed the Terrorist Attacks involving Plaintiffs.

953. Specifically, MOIS acted as a conduit for Iran's provision of funds, training and direction to Terrorist Group for their terrorist activities beyond the borders of Iran including the actions relating to the Terrorist Attacks and Plaintiffs' injuries.

954. MOIS and its agents have routinely been, and are presently designated by the U.S. Treasury as an SDN and SDGT, pursuant to Iranian Financial Sanctions Regulations ("IFSR"), including:

- a) Executive Order 13399 of April 25, 2006, *Blocking Property of Additional Persons in Connection With the National Emergency With Respect to Syria*, sanctioning entities and individuals that:

[H]ave been, involved in the planning, sponsoring, organizing, or perpetrating of: (A) the terrorist act in Beirut, Lebanon, that resulted in the assassination of former Lebanese Prime Minister Rafiq Hariri and the deaths of 22 others; or (B) any other bombing, assassination, or assassination attempt in Lebanon since October 1, 2004, that is related to Hariri's assassination or that implicates the Government of Syria or its officers or agents; (ii) to have obstructed or otherwise impeded the work of the Commission established pursuant to UNSCR 1595; (iii) to have materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services in support of, any such terrorist act, bombing, or assassination attempt, or any person designated pursuant to this order; or (iv) to be owned or controlled by, or acting or purporting to act for or on behalf of, directly or indirectly, any person designated pursuant to this order.

- b) Executive Order 13460 of February 13, 2008, *Blocking Property of Additional Persons in Connection With the National Emergency With Respect to Syria*, sanctioning entities and individuals:

[R]esponsible for or otherwise significantly contributing to actions taken or decisions made by the Government of Syria that have the purpose or effect of undermining efforts to stabilize Iraq or of

allowing the use of Syrian territory or facilities to undermine efforts to stabilize Iraq.

(Emphasis added).

- c) Executive Order 13553 of September 28, 2010, designating MOIS and its agents as an “IRAN-HR” entity, responsible for “serious human rights abuses by the government of Iran. In doing so the United States sought to sanction entities and individuals that:

[We’re] acting on behalf of the Government of Iran (including members of paramilitary organizations) who is responsible for or complicit in, or responsible for ordering, controlling, or otherwise directing, the commission of serious human rights abuses against persons in Iran or Iranian citizens or residents, or the family members of the foregoing, on or after June 12, 2009, regardless of whether such abuses occurred in Iran... materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, [such] activities described... or any person whose property and interests in property are blocked pursuant to this order; or.. owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order.

- d) Executive Order 13606 of April 22, 2012, designating MOIS and its agents as an “HRIT-IR” entity, responsible for “grave human rights abuses by the governments of Iran and Syria via information technology.” In doing so, the United States sanctioned entities and individuals that:

[P]rovided, directly or indirectly, goods, services, or technology to Iran or Syria likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran or Syria... [or] provided, directly or indirectly, goods, services, or technology to Iran or Syria likely to be used to facilitate computer or network disruption, monitoring, or tracking that could assist in or enable serious human rights abuses by or on behalf of the Government of Iran...[or] materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of [these] activities... [or] owned or controlled by, or to have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to this order.

955. MOIS has been involved in kidnappings, assassinations, and terrorism since its inception in 1985.

956. Many of the U.S. State Department reports on global terrorism over the last twenty-five years refer to MOIS as Iran's key facilitator and director of terrorist attacks.

957. In 1995 and again in 1996, Usama Bin Laden approached MOIS and asked to join forces against the United States. Bin Laden's phone records, obtained by U.S. investigators working on the U.S. embassy bombings in Kenya and Tanzania, show that 10 percent of phone calls made by Bin Laden and his lieutenants were to Iran.

958. Seif al-Adl, one of AQ's top-ranking leaders at the time, was the liaison between Iranians and AQ; he coordinated meetings with the IRGC's leaders and MOIS officials.

959. U.S. federal courts have consistently held that the IRGC and the MOIS are parts of the Iranian state itself.<sup>82</sup>

## **B. IRAN'S TERRORIST NETWORK IN IRAQ**

### **1. Ansar al Islam / Ansar al Sunna**

960. From its beginning, Iran did not confine its support of anti-U.S. national fighters to Shia groups. Iran also supported AAI, a radical terrorist group with close ties to al Qaeda.

961. AAI is a Kurdish Sunni Muslim insurgent group and separatist movement in Iraq with well-established ties to al-Qaeda and Iran.

962. Mullah Krekar, aka Faraj Ahmad Najmuddin, reportedly founded AAI in December 2001 (at that time, with funding and logistical support from al-Qaeda and Usama bin Laden, as well as support from Iran). However, the group has significant, life-sustaining ties to

---

<sup>82</sup> See e.g., *Rimkus v. Islamic Republic of Iran*, 575 F.Supp.2d 181, 198–200 (D.D.C. 2008) (Lamberth, C.J.); *Blais v. Islamic Republic of Iran*, 459 F.Supp.2d 40, 60–61 (D.D.C. 2006) (Lamberth, J.) (both MOIS and IRGC must be treated as the state of Iran itself for purposes of liability); and *Salazar v. Islamic Republic of Iran*, 370 F.Supp.2d 11, 105, 115–16 (D.D.C. 2005) (Bates, J.) (same).

Iran.

963. AAI seeks to transform Iraq into an Islamic state.

964. AAI has a number of aliases and/or subgroups, including Ansar al-Sunna; Ansar al-Sunna Army; Devotees of Islam; Followers of Islam in Kurdistan; Helpers of Islam; Jaish Ansar al-Sunna; Jund al-Islam; Kurdish Taliban; Kurdistan Supporters of Islam; Partisans of Islam; Soldiers of God; Soldiers of Islam; and Supporters of Islam in Kurdistan.

965. AAI seeks to expel western interests from Iraq and establish an independent Iraqi state based on its interpretation of Sharia law. AAI has been mostly active in the northern part of Iraq, western Iraq-Anbar province, and in the areas surrounding and including Mosul and Kirkuk since 2003.

966. In 2001, AAI seized control of several villages near the town of Halabja and established an administration ruled by Shari'a Law.

967. In late March 2003, the majority of AAI members fled across the border and regrouped in Iran with the assistance of the IRGC and the Iranian regime. Many of those fighters reentered Iraq and took active part in anti-Coalition activities. From Iran, the group continued to operate under Abu Abdullah Shafi's leadership and was temporarily renamed Ansar al-Sunna (although it officially re-adopted the name Ansar al-Islam in 2007).

968. Shortly after the U.S.-led invasion of Iraq in March 2003, the majority of AAI members were captured, killed, or fled to neighboring Iran. Mullah Krekar fled to Norway where he has remained ever since. In his place, Abu Abdullah al-Shafi, also known as Warba Holiri al-Kurdi, assumed command of the remnants of the organization. From Iran, the group continued to operate under Shafi's leadership and was temporarily renamed Ansar al-Sunna (it officially re-adopted the name AAI in 2007).

969. During the summer of 2004, the jihadists began migrating back into Iraq. A large number of the returning jihadists chose to settle in Mosul. In October 2004, Lt. Gen. Norton Schwartz, who at the time was the Director of the Joint Staffs at the Pentagon (and from 2008-2012 was Chief of Staff of the Air Force), warned that AAI had reemerged as the coalition's "principal organized terrorist adversary in Iraq."

970. From 2003-2007, AAI continued to target Coalition Forces and U.S. Nationals, including Plaintiffs. Its deadliest attack during this period occurred on February 1, 2004, when it launched multiple simultaneous suicide car bombings at PUK offices in Erbil, killing over 100 civilians and injuring over 130 more. By February 2007, AAI had claimed responsibility for over 1,600 attacks in Iraq, including against American nationals. AAI openly cooperated with al Qaeda in Iraq; however, it adamantly refused to formally join the Islamic State of Iraq, which was an umbrella organization established by al Qaeda in Iraq. Instead, in May 2007, AAI joined with the Mujahideen Army, the Islamic Army in Iraq, and Ansar al-Sunna Shariah (a splinter group that had broken from AAI in early 2007 because its members wished to take a harder line against al Qaeda in Iraq) to form an anti-Coalition umbrella organization called the Reformation and Jihad Front. The Reformation and Jihad Front was a pan-Islamist organization that challenged al Qaeda in Iraq for leadership of the Iraqi Sunni Islamist movement.

971. AAI claimed responsibility for the beheading of 12 Nepalese hostages and the kidnapping and beheading of an Iraqi who was employed as a mechanic for the American forces at the Mosul airport. AAI targeted Iraqi Kurds for alleged collaboration with the U.S. In September 2003, members of the Jaysch Ansar al-Sunna beheaded three Iraqi Kurdish militiamen in retaliation for the cooperation by Kurdish political parties with the U.S. in Iraq.

972. U.S. and British intelligence reports in 2004 "concluded that [AAI] was working

closely with Iran, and also al Qaeda, in its terrorist attacks against coalition forces.” One British defense report noted “Intelligence indicates that elements of Iran’s [IRGC-QF] ‘are providing safe haven and basic training to Iran-based [AAI] cadres.’” (Brackets in original).<sup>83</sup>

973. On December 21, 2004, AAI subgroup Jamaat Ansar al-Sunna launched a suicide bomb attack on FOB Marez in Mosul, Iraq. AAI insurgent Abu Museli, disguised as an Iraqi Security Services officer, entered the base mess tent and detonated the explosive vest he was wearing. The blast killed fourteen U.S. soldiers, four U.S. citizen Halliburton employees, and four Iraqi soldiers allied with the U.S. military. An additional fifty-one U.S. soldiers and twenty-one others sustained non-fatal injuries. AAI, through Jamaat Ansar al-Sunna, claimed credit for the attack. This Terrorist Attack resulted in the death, maiming, or injury of Plaintiffs.

974. Another British intelligence source “said that Iranian government agencies were also secretly helping [AAI] members cross into Iraq from Iran, as part of a plan to mount sniper attacks against coalition forces.”<sup>84</sup> American sources confirmed this information, adding that “an Iranian was aiding [AAI] ‘on how to build and set up’ IED’s.”<sup>85</sup>

975. In February 2004, Kurdish intelligence officials uncovered a cache of Syrian, Yemeni, and Saudi passports—all bearing Iranian entry stamps—in an AAI safe-house on the Iranian side of the border. The fact the passports found had Iranian stamps on them indicated the terrorists did not secretly infiltrate into Iran, but that they entered with the cognizance and full knowledge of the Iranian authorities. According to Iraqi intelligence officers, captured Ansar al-Sunna militants have admitted to receiving assistance from Iranian officials.

976. Iran played a significant role in supporting AAI. Iran openly allowed the group to

---

<sup>83</sup> Edward T. Pound, *Special Report: The Iran Connection*, U.S. News and World Report, Nov. 14, 2004.

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

operate along its borders despite the group's alleged affiliation with the al-Qaeda network. AAI was tasked with conducting checks on cars, leaving their stronghold to go into Iran, indicating coordination with the Islamic Republic.

977. According to a document from Iraqi intelligence dated June 13, 2002, and seized by U.S. forces in Iraq, a trust worthy source reported that Mullah Kraykar (Krekar), the head of the AAI organization arrived in Iran for negotiations with several Iranian officials. The information indicated the purpose of the visit was to confirm a unified strategy and to guarantee continuous Iranian support to that group.

978. According to other sources Mullah Krekar, spent many years in Iran and was arrested in Amsterdam after a flight from Tehran.

979. AAI operations decreased substantially by 2006, but the group continued to maintain an extensive support and financial infrastructure in Europe that it used to recruit and send jihadists to Iraq.

980. Over the course of 2007-2008, AAI moved increasingly away from the Reformation and Jihad Front and strengthened its ties to al Qaeda in Iraq. It coordinated with al Qaeda in Iraq on several attacks against U.S. and PUK troops and began to adopt al Qaeda in Iraq's hardline attitude against Sunni Iraqis who worked for the U.S. or Iraqi governments.

981. On May 4, 2010, AAI's leader Abu Abdullah al-Shafi was captured and imprisoned by U.S. forces in Baghdad. On December 15, 2011, AAI announced a new leader: Abu Hashim Muhammad bin Abdul Rahman al Ibrahim.

982. AAI conducted attacks against a wide range of targets including Iraqi government and security forces, as well as U.S. and Coalition Forces and U.S. nationals, including Plaintiffs. AAI has conducted numerous kidnappings, executions, and assassinations of Iraqi citizens and

politicians. The group has either claimed responsibility or is believed to be responsible for attacks in 2011 that resulted in 24 deaths and 147 wounded.

983. On February 19, 2003, The Bank of England ordered British financial institutions to freeze AAI assets.

984. The U.S. Department of Treasury designated AAI a SDT under E.O 13224 on February 20, 2003. The U.S. Department of State designated AAI a FTO on March 22, 2004.

985. The United Nations Security Council Resolution 1267 Committee designated AAI as an Al-Qaida affiliate pursuant to UNCSRs 1267, 1390, and 1455 on February 27, 2003. The resolutions subjected it to the following sanctions:

**ARMS EMBARGO:** Prevent the direct or indirect supply, sale, and transfer from their territories or by their nationals outside their territories, or using their flag vessels or aircraft, of arms and related materiel of all types, spare parts and technical advice, assistance, or training related to military activities, to designated individuals and entities.

**ASSETS FREEZE:** Freeze without delay the funds and other financial assets or economic resources of designated individuals and entities, ensure that no funds, financial assets or economic resources are made available, directly or indirectly for their benefit.

986. Australia, New Zealand, Canada, and the European Union have designated AAI as terrorist organization. The U.S. Treasury Department designated Mullah Krekar as an individual providing assistance to terrorism and thus subject to having all international assets frozen in December 2006.

987. As such, AAI required alternate and clandestine sources of U.S. currency to continue its terror operations in Iraq. This source was Iran.

## 2. Special Groups

988. Iran opposed U.S. peacekeeping efforts and initiated acts of international terrorism against U.S. nationals, Coalition Forces, and Iraqi citizens with the goals of destabilizing Iraq and increasing Iranian influence in that country.

989. Iran's support for the Special Groups is both clear and disturbing. The IRGC-QF attempted to develop the Special Groups into a network similar to Hezbollah – a highly-lethal network that relied upon the Iranian regime to survive.<sup>86</sup> The purpose of the IRGC-QF in developing these Special Groups was to create highly lethal networks that relied upon the Iranian regime to survive, and thus, were controlled, either directly or indirectly, by Iran.

990. Iran leveraged (and continues to do so) its control and dominion over the IRGC, the IRGC-QF, and Hezbollah, and through those entities, provided the Special Groups with training (in Iran), weapons, safe harbor, U.S. currency, and intelligence, including those Special Groups responsible for the Terrorist Attacks which killed, maimed, or otherwise injured Plaintiffs.<sup>87</sup> The training provided to the Special Groups while they were in Iran included tactics and technology to conduct kidnappings, small unit tactical operations, and employ sophisticated IEDs.<sup>88</sup>

991. These Special Groups returned to Iraq after receiving their Iran-supported training, maintaining their group's organization. Thus, each Special Group consisted of Iraqi civilians who train together in Iran on how to use IEDs, EFPs, mortars, rockets, as well as intelligence, sniper, and kidnapping operations.<sup>89</sup>

992. The Special Groups operate throughout Iraq and, at all relevant times, remained under the control of Iran, through its Agents and Proxies, the IRGC, the IRGC-QF, and Hezbollah.

---

<sup>86</sup> Press Briefing by Multi-National Force-Iraq Deputy Chief of Staff for Strategic Effects Brigadier General Kevin Bergner, Security Operations in Iraq.

<sup>87</sup> U.S. Department of Defense, *CDA—Military Power of Iran, Unclassified Report on Military Power of Iran* (Apr. 2010), [http://www.fas.org/man/eprint/dod\\_iran\\_2010.pdf](http://www.fas.org/man/eprint/dod_iran_2010.pdf).

<sup>88</sup> U.S. Department of Defense, *Iranian Government Behind Shipping Weapons to Iraq* (Sept. 28, 2006), <http://www.defense.gov/news/newsarticle.aspx?id=1289>.

<sup>89</sup> July 2, 2007 Press Briefing by Brigadier General Kevin Bergner.

993. Utilizing the training, weapons, and funding provided by Defendants, either directly or indirectly, the Special Groups planned and executed a string of bombings, kidnappings, sectarian murders, and more against Iraqi civilians, Coalition Forces, and U.S. nationals, including Plaintiffs.

994. Although U.S. policy (supported by U.N. Security Council resolutions) was to establish peace and stability in Iraq in the hopes of establishing a democratic government, Iran viewed the U.S. and international peacekeeping efforts in Iraq as a potential threat to its regime.

995. Rather than cooperate with the United States and Coalition Forces authorized by the U.N. to bring peace, democracy, and stability to Iran, or alternatively, Iran chose to undermine U.S. and U.N. peacekeeping efforts by unleashing massive waves of terrorism and sectarian violence in Iraq and, in part, by targeting U.S. Nationals, including Plaintiffs, through the Special Groups that Iran controlled.

996. President Bush declared on May 1, 2003, that “major combat operations in Iraq have ended.”

997. The U.N. Security Council authorized the post-conflict occupation of Iraq by Coalition Forces in October 2003 to maintain “security and stability.” S.C. Res. 1511, ¶ 13, U.N. Doc. S/RES/1511 (Oct. 16, 2003).

998. After 2003, the IRGC inserted hundreds of its Iranian-trained operatives into Iraq’s state security organs (notably the Ministry of Interior intelligence structure) in part through its influence within the Badr Organization (discussed further below).

999. In addition to its coordination with the Badr Organization, Iran, through the IRGC-QF, formed the Ramezan Corps intended to operate specifically in Iraq.

1000. The Ramezan Corps cultivated, armed, trained, and supported several Shi'a terror

groups in Iraq the U.S. military later termed “Special Groups.”

1001. Although a June 7, 2004 U.N. Security Council Resolution (S.C. Res. 1546, U.N. Doc. S/RES/1546) expressly assigned Coalition Forces in Iraq the task of helping Iraq “*by preventing and deterring terrorism*,” Iran set out to target Coalition Forces and U.S. nationals, including Plaintiffs, and force them out of Iraq.

1002. After Coalition Forces arrived in Iraq, Iranian intelligence services penetrated Iraq rapidly and thoroughly. The thrust of their surveillance efforts was finding out what weapons U.S. troops were carrying and what kind of body armor they were wearing. Iranian agents also sought information on the location of U.S. Army and intelligence bases; on the routes traveled by U.S. convoys; on the operations of the Special Forces’ elite Delta Force; and on the plans of the U.S. military and intelligence inside Iraq. The Iranians offered U.S. Dollar bounties to Iraqis for killing Americans, shooting down U.S. helicopters, and destroying American tanks.

1003. The number and sophistication of Special Groups increased in 2005.

1004. In 2007, the Special Groups further escalated the number of mortar and rocket attacks against U.S. national targets, including Plaintiffs, in the Baghdad International Zone. The accuracy of this indirect fire improved because of the training and weapons these Special Groups received from Iran.<sup>90</sup>

1005. In summary, from October 2003 onward, even though U.S. military personnel in Iraq were participants in an internationally recognized peace keeping mission, Iran embarked on a policy of terrorism, extrajudicial killings and murder, kidnapping and torture to thwart those efforts.

---

<sup>90</sup> U.S. Department of Defense Special Briefing by Lieutenant General Ray Odierno, U.S. Army, Commander, Multi-National Corps-Iraq, *Operation Phantom Thunder* (June 22, 2007).

1006. Because of the perceived unreliability and value of the post-Hussein regime Iraqi currency, Special Groups and other terrorists in Iraq used U.S. currency almost exclusively.

1007. Iran facilitated and enabled the terrorist attacks launched against U.S. Nationals, including the Plaintiffs, and others on a massive scale which would not have been possible without the provision of hundreds of thousands of munitions, advanced technologies, training, funding, intelligence, safe harbor, and other material support detailed herein.

1008. Without the massive Iranian funding and material support, Special Groups and other Iranian Agents and Proxies would not have been able to conduct the thousands of acts of international terrorism on the scale and with the lethality they achieved, including the Terrorist Attacks which resulted in the deaths, maiming, or otherwise injuring of Plaintiffs and Plaintiffs' family members.<sup>91</sup>

### **3. The Badr Corps/Badr Organization**

1009. The Badr Corps was established in 1982 in Iran as the military wing of the Supreme Council for Islamic Revolution in Iraq.

1010. From its headquarters in Iran, the Badr Corps operated extensive networks throughout Iraq in the 1990s. The group smuggled men and weapons into Iraq to conduct attacks against the Iraqi regime of Saddam Hussein.

1011. Like Hezbollah, the Badr Corps established clandestine offices in businesses and social organizations in Iraq.

1012. The Badr Corps also used Iraqi front companies to recruit operatives, collect intelligence, and circulate propaganda materials in Shi'a populated areas.

1013. Before 2003, the Badr Corps served as Iran's most important surrogate inside

---

<sup>91</sup> July 2, 2007 Press Briefing by Brigadier General Kevin Bergner.

Iraq, acting as a *de facto* arm of the IRGC-QF.

1014. The Badr Corps received training and weapons from Iraq through the IRGC and Hezbollah.

1015. After Saddam Hussein's overthrow, the Badr Corps renamed itself the Badr Organization, and many of its operatives joined the newly formed Iraqi security forces.

1016. Published reports indicate that thousands of members of the Badr Organization remained on the IRGC-QF payroll after 2004.

1017. Several senior BADR Corps operatives later emerged as key conduits for funneling weapons to Iranian Agents and Proxies and the Terrorist Groups in Iraq from 2004 through at least 2011, including Abu Mustafa al-Sheibani, a key smuggler of deadly Iranian IEDs, and Jamal Ja'far Muhammad, a/k/a Abu Mahdi al-Muhandis (a/k/a "The Engineer"), who later led KH.

1018. "Department 1000" of the IRGC-QF, known as the Ramezan Corps, is in charge of Iraqi operations and remains the largest IRGC-QF command outside of Iran. It coordinated, armed, and influenced the Badr Organization.

1019. Although the Badr Organization evolved into a major political organization with seats in the new Iraqi parliament, it also played a significant role in facilitating Special Groups' operations in Iraq. A number of Special Groups commanders such as Al-Muhandis are, or were, Badr Corp agents and operatives.

1020. Through the Badr Corp the IRGC inserted hundreds of its Iranian-trained operatives into Iraq's state security organs (e.g. the Iraqi Ministry of Interior Intelligence structure) during the Relevant Period.

#### **4. Kata'ib Hizbollah**

1021. KH has functioned as Iran's go-to terror group in Iraq and received support from

Iranian-funded Lebanese Hezbollah, including training in weapons use; IED construction and operation; and sniper, rocket, and mortar attacks. KH is a radical Shia Islamist group, an Iraqi terrorist organization, and an anti-Western establishment responsible for numerous terrorist acts against Iraqi, U.S., and other targets in Iraq since 2007. KH has ideological ties to Lebanese Hezbollah.

1022. KH has a number of aliases, including Hezbollah Brigades; Hezbollah Brigades in Iraq; Hezbollah Brigades-Iraq; KH; Kata 'ib Hezbollah; Kheta'ib Hezbollah; Khattab Hezbollah; Hezbollah Brigades-Iraq of the Islamic Resistance in Iraq; Islamic Resistance in Iraq; Kata'ib Hizbullah Fi al-Iraq; Katibat Abu Fathel al-A'abas; Katibat Zayd Ebin Ali; and Katibat Karbalah.

1023. KH was formed in 2006 and came to prominence in 2007 for attacks against Coalition Forces and U.S. nationals, including Plaintiffs, and its online propagandizing of those attacks. The IRGC-QF established it as a vehicle to deploy its most experienced operators and its most sensitive equipment. Historically, KH operated mainly in Shi'a areas of Baghdad, such as Sadr City, and throughout the south.

1024. The IRGC-QF positioned one of its own, Abu Mahdi al-Muhandis, as the leader of KH. Under al-Muhandis, KH developed as a compact movement of less than 400 personnel that is firmly under IRGC-QF control and maintains relatively good operational security.

1025. In June 2011, five U.S. soldiers were killed in a rocket attack in Baghdad when KH assailants fired between three and five rockets at U.S. military base Camp Victory.

1026. On June 24, 2009, the United States designated KH an FTO.

1027. The State Department's notice of KH's FTO designation stated that:

The organization has been responsible for numerous violent terrorist attacks since 2007, including improvised explosive device bombings, rocket propelled grenade

attacks, and sniper operations. Kata'ib Hizballah [sic] also targeted the International Zone in Baghdad in a November 29, 2008 rocket attack that killed two UN workers. In addition, KH has threatened the lives of Iraqi politicians and civilians that support the legitimate political process in Iraq.

1028. KH was simultaneously designated an SDGT under E.O. 13224, because it was “responsible for numerous terrorist acts against Iraqi, U.S., and other targets in Iraq since 2007.”

1029. The U.S. Treasury Department also designated KH pursuant to E.O. 13438. The Treasury Department’s 2009 press release announcing KH’s designation explained that KH had “committed, directed, supported, or posed a significant risk of committing acts of violence against Coalition and Iraqi Security Forces....” The press release also quoted then-Under Secretary for Terrorism and Financial Intelligence Stuart Levey as stating “[t]hese designations play a critical role in our efforts to protect Coalition troops, Iraqi security forces, and civilians from those who use violence against innocents to intimidate and to undermine a free and prosperous Iraq.” The Treasury press release also stated: “[f]urther, the IRGC-Qods Force provides lethal support to KH and other Iraqi Shia militia groups who target and kill Coalition and Iraqi Security Forces.” The 2009 press release further reported that between March 2007 and June 2008, KH led a number of attacks against U.S. forces in Iraq, advising:

As of 2008, Kata'ib Hizballah was funded by the IRGC-Qods Force and received weapons training and support from Lebanon-based Hizballah. In one instance, Hizballah provided training--to include building and planting IEDs and training in coordinating small and medium arms attacks, sniper attacks, mortar attacks, and rocket attacks--to Kata'ib Hizballah members in Iran.

1030. Furthermore, the 2009 U.S. Treasury Department press release noted:

Recordings made by Kata'ib Hizballah for release to the public as propaganda videos further demonstrate that Kata'ib Hizballah conducted attacks against Coalition Forces. In mid-August 2008, Coalition Forces seized four hard drives from a storage facility associated with a Kata'ib Hizballah media facilitator. The four hard drives included approximately 1,200 videos showing Kata'ib Hizballah’s sophisticated planning and attack tactics, techniques, and procedures, and Kata'ib Hizballah’s use of the most lethal weapons--including RPG-29s,

IRAMs, and EFPs--against Coalition Forces in Iraq.

1031. One of the hard drives contained 35 attack videos edited with the KH logo in the top right corner. Additionally, between February and September 2008, Al-Manar in Beirut, Lebanon, broadcast several videos showing KH conducting multiple attacks against U.S. nationals and Coalition Forces in Iraq.

1032. Immediately preceding the Government of Iraq's approval of the United States-Iraq security agreement in late November 2008, KH posted a statement that the group would continue fighting Coalition Forces and threatened to conduct attacks against the Government of Iraq if it signed the security agreement with the United States.

1033. In 2008, the U.S. Department of Defense described the links between KH, Iran, and multiple terrorist attacks against U.S. nationals in Iraq—including KH's use of EFPs:

[A]lso known as Hezbollah Brigades, is a terrorist group believed to receive funding, training, logistics, and material support from Iran to attack Iraqi and coalition forces using what the military calls 'explosively formed penetrators' – roadside bombs designed to pierce armor-hulled vehicles – and other weapons such as rocket-assisted mortars.

1034. As noted above—and as stated by the U.S. Treasury Department in its July 2009 press release—throughout 2008, Al-Manar, Lebanon Hezbollah's official television outlet in Lebanon (and itself a designated SDGT since May 2006), played numerous videos of KH launching rocket and IED attacks against U.S. troops. In this manner, Hezbollah helped publicize KH's activities and increase its profile among leading Shi'a terrorist groups.

1035. Although KH's leadership remains in flux, one individual reportedly associated with the group is Abu Mahdi al-Muhandis. According to an inquiry published by Kuwaiti daily

al-Rai on June 4 2016, during the 80's, Abu Mahdi al-Muhandis received an Iranian citizenship from the Iranian regime as part of his prominent role in the Badr Corps.<sup>92</sup>

1036. KH's leader, Abu Mahdi al-Muhandis, is wanted in Kuwait for his alleged role in the 1983 bombings of the American and French embassies in Kuwait City, as well as for his alleged involvement in the assassination attempt on the Kuwaiti Emir in 1985. In an interview to Hezbollah-affiliated media on January 3, 2017, Abu Mahdi al-Muhandis admitted that he cooperated with Hezbollah top commanders Imad Moughniyah and Mustafa Badreddine from the early 80's. According to him, this cooperation included training opposition Iraqi Shiite groups to fight Saddam Hussein regime and the U.S. troops in Iraq beginning in 2003.<sup>93</sup>

1037. The U.S. Treasury Department designated al-Muhandis an SDGT in July 2009, and announced the designation in the same press release announcing KH's designation. That press release stated:

As of early 2007, al-Muhandis formed a Shia militia group employing instructors from Hizballah to prepare this group and certain Jaysh al- Mahdi (JAM) Special Groups for attacks against Coalition Forces. The groups received training in guerilla warfare, handling bombs and explosives, and employing weapons--to include missiles, mortars, and sniper rifles. In another instance as of September 2007, al-Muhandis led networks that moved ammunition and weapons--to include explosively formed penetrators (EFPs)--from Iran to Iraq, distributing them to certain JAM militias to target Coalition Forces. As of mid-February 2007, al-Muhandis also ran a weapons smuggling network that moved sniper rifles through the Iran-Iraq border to Shia militias that targeted Coalition Forces. Al-Muhandis also provided logistical support for attacks against Iraqi Security Forces and Coalition Forces conducted by JAM Special Groups and certain Shia militias. In one instance, in April 2008, al-Muhandis facilitated the entry of trucks--containing mortars, Katyusha rockets, EFPs, and other explosive devices--from Iran to Iraq that were then delivered to JAM Special Groups in Sadr City,

---

<sup>92</sup> See <http://www.alraimedia.com/ar/article/special-reports/2016/06/04/684698/nr/nc> (last visited Oct. 14, 2017) (Arabic translation available).

<sup>93</sup> See Middle East Media Research Institute TV Monitor Project, Clip #5829, <https://www.memri.org/tv/abu-mahdi-al-muhandis-deputy-commander-popular-mobilization-units-optimism-over-liberation-mosul> (last visited Oct. 14, 2017).

Baghdad. Additionally, al- Muhandis organized numerous weapons shipments to supply JAM Special Groups who were fighting Iraqi Security Forces in the Basrah and Maysan provinces during late March-early April 2008.

In addition to facilitating weapons shipments to JAM Special Groups and certain Shia militias, al-Muhandis facilitated the movement and training of Iraq-based Shia militia members to prepare them to attack Coalition Forces. In one instance in November 2007, al-Muhandis sent JAM Special Groups members to Iran to undergo a training course in using sniper rifles. Upon completion of the training course, the JAM Special Groups members had planned to return to Iraq and carry out special operations against Coalition Forces. Additionally, in early March 2007, al-Muhandis sent certain Shia militia members to Iran for training in guerilla warfare, light arms, marksmanship, improvised explosive devices (IED) and anti-aircraft missiles to increase the combat ability of the militias to fight Coalition Forces.

In addition to the reasons for which he is being designated today, al-Muhandis participated in the bombing of Western embassies in Kuwait and the attempted assassination of the Emir of Kuwait in the early 1980s. Al-Muhandis was subsequently convicted in absentia by the Kuwaiti government for his role in the bombing and attempted assassination.

1038. In a July 2010 press briefing, U.S. General Ray Odierno identified KH as the group behind increased threats to U.S. bases in Iraq. General Odierno confirmed that KH operatives had gone to Iran for special training and then returned to Iraq. General Odierno stated, “[T]hey are clearly connected to Iranian IRGC.”

##### **5. Jaysch al Mahdi and The Promised Day Brigades**

1039. JAM was established by radical Shi'a cleric Muqtada al-Sadr in June 2003. On April 18, 2004, it led the first major armed confrontation by Shi'a militia against U.S.-led forces in Iraq.

1040. JAM was co-founded by Imad Mughnayih, once the terrorism chief of Hezbollah and “an agent of Iran and a direct role in Iran’s sponsorship of terrorist activities.”<sup>94</sup> Prior to

---

<sup>94</sup> “Imad Fayed Mughnayih (a/k/a Hajj Radwan) was, for decades prior to his death in February 2008, the terrorist operations chief of Hizballah. Mughnayih played a critical role in a series of imaginative high-profile

September 11, 2001, Mughniyah was ranked number one on the FBI's most wanted list for leading the attacks which killed 183 Marines in the bombing of the Holiday Inn in Beirut, the hijacking of a TWA plane and murder of a U.S. Navy diver, and the bombing of the U.S. Embassy in Beirut (replaced as number one most wanted by Usama bin Laden).

1041. In Iraq, JAM expanded its territorial control of mixed or predominantly Shi'a neighborhoods and displaced or killed the local Sunni population.

1042. JAM was able to gain initial control in many of the neighborhoods in and around Baghdad (such as Sadr City) by offering the Shi'a population protection and social services.

1043. In a Department of Defense news briefing on August 24, 2007, General Rick Lynch confirmed that on August 7, 2006, the 3<sup>rd</sup> Brigade Combat Team "conducted a raid on a militant house . . . about 20 miles east of Baghdad . . . They arrested one of our division's most valued targets, . . . [who] acted as a link between Iran and the [JAM]. He was the main Shia conduit in that region for getting Iranian EFPs and rockets into Baghdad, . . ."<sup>95</sup>

1044. Al-Sadr dissolved part of his militia after 2007, but maintained a small group of Iranian-supported militants called the PDB to carry out terrorist attacks against Coalition Forces and U.S. nationals, including certain Plaintiffs.

1045. The PDB has received funding, training, and weapons from the IRGC and is one of the Special Groups.

1046. The PDB actively targeted U.S. nationals, including Plaintiffs and U.S. forces, in

---

terrorist attacks across the globe, and his abilities as a terrorist coordinator, director, and operative was an order of magnitude beyond anything comparable on the scene between 1980-2008.

Mughniyah was, since the early 1980s, an agent of the Islamic Republic of Iran, where he lived for many years. Imad Mughniyah had a direct reporting relationship to Iranian intelligence and a direct role in Iran's sponsorship of terrorist activities." *In re Terrorist Attacks on September 11, 2001*, 2011 U.S. Dist. LEXIS 155899, at \*106-07.

<sup>95</sup> KIMBERLY KAGAN, THE SURGE: A MILITARY HISTORY (ENCOUNTER BROADSIDES) (2010).

an attempt to disrupt security operations and further destabilize Iraq.

1047. For example, on June 28, 2011, the PDB issued a statement claiming responsibility for ten (10) mortar and Katyusha rocket attacks against U.S. Military convoys in which U.S. officials confirmed that three U.S. troops were killed.

#### **6. Asa'ib Ahl Al-Haq**

1048. Asa'ib Ahl Al Haq (or the “League of the Righteous”) terrorist organization is a Shi'a Special Group supported by Hezbollah and the IRGC-QF that conducted assassinations and operations in Iraq against Coalition Forces and various individuals and U.S. nationals.

1049. AAH was originally established by Senior Sadrists and MDF-I detainee Qais al-Khazali. His brother, Laith Khazali, also helped lead the organization.

1050. AAH split from al-Sadr's JAM in 2006. Since that time, AAH has conducted: thousands of IED attacks against U.S. and Iraqi forces; targeted kidnappings of Westerners and Iraqis; rocket and mortar attacks on the U.S. Embassy; murders of American and British soldiers; and assassinations of Iraqi officials.

1051. During the Relevant Period, AAH received significant funding from Iran, and had links to Iran's IRGC-QF and Hezbollah.

1052. Senior Lebanese Hezbollah operative Ali Musa Daqduq provided training to AAH terrorists.

1053. Daqduq reported to Youssef Hashim, the head of Lebanese Hezbollah Special Operations, and the latter reported to Abdul Reza Shahlai, the director of the IRGC-QF External Operations.

1054. Hezbollah and the IRGC-QF provided JAM, PDB, KH, AAH, and other Shi'a groups with a variety of weapons and training used to target U.S. nationals, including Plaintiffs, and Coalition Forces engaged in their post-2003 peacekeeping mission.

1055. These weapons included signature Iranian munitions such as EFPs and IRAMs, as well as 107 mm rockets (often used as part of IRAMs), 120 mm and 60 mm mortars, RPG launchers and other small arms.

1056. The training provided by Iran and its Agents and Proxies to the Terrorist Groups resulted in an increased lethality and effectiveness of the Terrorist Attacks, and included sophisticated tell-tale tactics that had not previously been seen in Iraq prior to infusion of Iranian agents, Hezbollah, and the IRGC-QF in 2003.

## **7. Al Qaeda**

1057. Al Qaeda is a designated international terrorist organization, widely recognized as such by all civilized nations and the United Nations, and is not a legitimate “*military force*” nor a recognized sovereign state.

1058. The United States has designated al Qaeda, including its branches, subsidiaries and “franchisees” (including al-Qaeda in Iraq) as a FTO and a SDGT.

1059. Commencing in the early 1990s and continuing until at least 2011, Iran and Sudan provided al Qaeda significant indispensable funding, weapons, safe haven, training, intelligence, passports, and centers for command and control. Iran also provided undocumented transport between Afghanistan, Iraq and Pakistan across its borders and other significant material support.

1060. In the 1990s, al Qaeda developed a close relationship with Iran and the IRGC. Usama bin Laden and Ayman al Zawahiri held clandestine meetings with Imad Mughnayih and Ahmad Vahidi (then commander of IRGC Qods Force) which “lead to an informal agreement to cooperate in providing support for actions carried out primarily against Israel and the United States...Thereafter, senior al Qaeda operatives and trainers traveled to Iran to receive training in

explosives. Usama bin Laden also sent senior aides to Iran for training with the IRGC and to Lebanon for training with Hizballah.”<sup>96</sup>

1061. On June 30, 1989, General Omar Hassan al-Bashir led a coup d'état toppling the exiting regime in Sudan. The radical Salafi cleric, Hassan Abd Allah al Turabi served as the “intellectual architect,” or “the power behind the throne,” sometimes officially as leader of the National Islamic Front and sometimes as speaker of the parliamentary assembly.

1062. In 1990-1991, Turabi founded the Popular Arab and Islamic Congress, which included representatives from the Palestine Liberation Organization, Hamas, Egyptian Islamic Jihad, al Qaeda, Algerian Islamic Jihad, Hezbollah, Abu Nidal Group, and the Islamic Revolutionary Guard Corp.

1063. In 1991, the Kingdom of Saudi Arabia expelled al Qaeda leader Usama bin Laden (“UBL”) and UBL moved his base of operations to Sudan.

1064. The Sudanese army protected Bin Laden’s home in Khartoum and his terrorist training bases within the country as well as providing al Qaeda with access to the international and United States financial networks. In addition, Sudan provided al Qaeda with 200 Sudanese passports, allowing al Qaeda operatives to travel under fictitious identities.

1065. Turabi brought together UBL and leaders of the IRGC-QF and leaders of Hezbollah. Commencing in April, 1991, Turabi hosted meetings bringing together leaders from al Qaeda, Hezbollah and Iranian and Sudanese officials. According to al Qaeda shura council member Abu Hajar al-Iraqi, the purpose of these meetings was to focus on common enemies, the West and the United States.

1066. In 1991, Hezbollah opened a base of operations in Khartoum, Sudan.

---

<sup>96</sup> *In re Terrorist Attacks on September 11, 2001*, 2011 U.S. Dist. LEXIS 155899, at \*110–11.

1067. On December 13, 1991, Iranian President Ali Akbar Hashemi Rafsanjani arrived in Khartoum, Sudan for a six-day visit, by a delegation of 157 members, including Mohsen Rezai then Commander of the IRGC, Iranian Intelligence Minister Ali Fallahian and Iranian Defense Minister Ali Akbar Torkan. Various agreements were signed between Iran and Sudan, pursuant to which, *inter alia*, Iran delivered \$300 million of Chinese weapons and 2,000 IRGC operatives were sent to train Sudan's Popular Defense Forces.

1068. According to the 9/11 Commission Report, in late 1991 or 1992, discussions in Sudan between al Qaeda and Iranian operatives led to an agreement to cooperate in providing support - specifically, training - for actions carried out primarily against Israel and the United States. Not long afterward, senior al Qaeda operatives and trainers traveled to Iran to receive training in explosives.

1069. The 9/11 Commission reported that “[t]he relationship between al Qaeda and Iran demonstrated that Sunni-Shia divisions did not necessarily pose an insurmountable barrier to cooperation in terrorist operations.”<sup>97</sup>

1070. Iran was a valuable connection for UBL and al Qaeda, and al Qaeda was highly beneficial to Iran, given al Qaeda's extreme and violent position against America and its animosity against the Kingdom of Saudi Arabia. Iran, and Hezbollah played significant roles in the buildup of al Qaeda's terrorist capabilities.

1071. As a result of the creation of this terrorist alliance, al Qaeda leader Ayman al Zawahiri repeatedly visited Tehran during the 1990s and met with Minister Ali Fallahian and other officers of MOIS, and IRGC-QF Commander Ahmad Vahidi.

---

<sup>97</sup> The National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report*, p. 61 (July 22, 2004), <https://govinfo.library.unt.edu/911/report/911Report.pdf>.

1072. Throughout the 1990s, the al Qaeda-Iran-Hezbollah terrorist training arrangement continued. Hezbollah leader Imad Mughnayih coordinated these training activities, including training of al Qaeda personnel, with Iranian government officials in Iran and with IRGC officers working undercover at the Iranian embassy in Beirut, Lebanon.

1073. Al Qaeda operative Ali Mohammed provided security for one prominent meeting between Hezbollah's chief external operations officer, Imad Mughnayih, and Bin Laden in Sudan. Mohammed testified at his plea hearing that "*Hezbollah provided explosives training for al Qaeda and al Jihad. Iran supplied Egyptian Jihad with weapons. Iran also used Hezbollah to supply explosives that were disguised to look like rocks.*"

1074. Iran trained Saif al-Adel, head of al Qaeda security, and other al Qaeda members, including shura council members, at Hezbollah training camps in the mid-1990s. Al Qaeda leader Mustafa Hamid was one of al Qaeda's primary points of contact with IRGC. He negotiated the agreement between al Qaeda and Iran, which secured safe transit between Iran and Afghanistan and to Iraq for al Qaeda members.

1075. These training camps were used by al Qaeda in planning and perpetrating the terrorist attacks conducted against U.S. civilians, diplomats, and servicemen and women, such as: the suicide bombing of U.S. Air Force personnel and their families in Khobar, Saudi Arabia; the U.S. embassies in Nairobi and Dar es Salaam; and the World Trade Center on September 11, 2001.

1076. On June 25, 1996, Iranian-backed Hezbollah terrorists, with the support of al Qaeda, bombed the Khobar Towers housing complex in Dhahran, Saudi Arabia, killing 19 U.S. servicemen and wounding approximately 500 others. FBI investigators concluded: the operation was undertaken on direct orders from senior Iranian government leaders; the bombers had been

trained and funded by the IRGC in Lebanon's Bekaa Valley; and senior members of the Iranian government, including Ministry of Defense, Ministry of Intelligence and Security and the Supreme Leader's office, had selected Khobar as the target and commissioned Hezbollah to carry out the operation.

1077. Al Qaeda was involved in the planning and preparations for the Khobar Towers bombing. Usama bin Laden tried to facilitate a shipment of explosives to Saudi Arabia, and, on the day of the operation, bin Laden was, according to NSA intercepts, congratulated on the telephone.<sup>98</sup>

1078. The 9/11 Commission examined classified CIA documents establishing that IRGC-QF commander Ahmad Vahidi planned the Khobar Towers attack with Ahmad al Mugassil, a Saudi-born al Qaeda operative.

1079. Iran aided, abetted and conspired with Hezbollah, Osama Bin Laden, and al Qaeda to launch the large-scale bombing attacks against the United States embassies in Nairobi and Dar es Salaam on August 7, 1998. Prior to their meetings with Iranian officials and agents, Bin Laden and al Qaeda did not possess the technical expertise required to carry out the embassy bombings. The Iranian defendants, through Hezbollah, provided explosives training to Bin Laden and al Qaeda and rendered direct assistance to al Qaeda operatives.<sup>99</sup>

1080. As stated in the 9/11 Report, "Iran made a concerted effort to strengthen relations with al Qaeda after the October 2000 attack on the *USS Cole...*" For example, Iranian officials facilitated the travel of al Qaeda members – including at least 8 of the 9/11 hijackers – through

---

<sup>98</sup> *Id.* at 60.

<sup>99</sup> Owens v Republic of Sudan, 826 F. Supp. 2d 128, 139. D.D.C. 2011

Iran on their way to and from Afghanistan, where the hijackers trained at al Qaeda's terrorist training camps.<sup>100</sup>

1081. U.S., Saudi, and Egyptian political pressure on the Sudanese eventually forced them to expel Usama bin Laden in May 1996. Radical Afghan Sunni warlord Gulbuddin Hekmatyar, a strong Iranian ally, invited bin Laden to join him in Afghanistan. Usama bin Laden then relocated to Afghanistan with the assistance of the Iranian intelligence services.<sup>101</sup>

1082. Iran provided material support to al Qaeda after the 9/11 attacks in several ways, most significantly by providing safe haven to al Qaeda leaders and operatives, keeping them safe from retaliation by U.S. forces, which invaded Afghanistan. According to the U.S. Treasury Department press release on January 16, 2009, in late 2001, while in Tehran, al Qaeda senior operative Mustafa Hamid negotiated with the Iranians to relocate al Qaeda families to Iran after the 9/11 attacks.

1083. In the fall of 2001, Iran facilitated the exit from Afghanistan, into Iran, of numerous al Qaeda leaders, operatives, and their families. The Iran-Afghanistan safe passageway, established earlier to get al Qaeda recruits into and out of the training camps in Afghanistan, was utilized to evacuate hundreds of al Qaeda fighters and their families from Afghanistan into Iran for safe haven there. The IRGC knew of, and facilitated, the border crossings of these al Qaeda fighters and their families entering Iran.

1084. Among the high-level al Qaeda officials who arrived in Iran from Afghanistan at this time were Saad bin Laden and the man who would soon lead "al Qaeda in Iraq," Abu Musab al Zarqawi.

---

<sup>100</sup> *Id.* at 240-41.

<sup>101</sup> *Id.* at 65.

1085. In late 2001, Sa'ad bin Laden facilitated the travel of Usama bin Laden's family members from Afghanistan to Iran. Thereafter, Sa'ad bin Laden made key decisions for al Qaeda and was part of a small group of al Qaeda members involved in managing al Qaeda from Iran.

1086. By 2002, al Qaeda had established in Iran its 'management council,' a body that bin Laden reportedly tasked with providing strategic support to the organization's leaders in Pakistan. Key members of the council included Saif al-Adel, Sulayman Abu Ghayth, Abu al-Khayr al-Masri, Abu Muhammad al-Masri, and Mahfouz Ould al-Walid (a.k.a. Abu Hafs al-Mauritani). All five senior operators remained influential over the next several years and retained close ties to bin Laden. Adel organized groups of fighters to overthrow Hamid Karzai's regime in Afghanistan and provided support for the May 12, 2003 terrorist attacks in Riyadh.<sup>102</sup>

1087. The Iranian regime offered al Qaeda this safe haven in order to advance its own interests. Having al Qaeda operatives in the country gave Iran a bargaining chip and important leverage with the U.S. and Saudi Arabia. In addition, it enabled Iran to protect itself from a possible attack against targets in Iran. The deal enabled Iran to cause chaos in Iraq and thus preventing it from becoming a Muslim democratic regime, which would endanger the security of the Iranian regime by the example and influence it would pose to the tens of thousands of Iranian pilgrims who visit the Shiite shrines in Iraq each year.

1088. The deal was reportedly reached between IRGC-QF commander Qassem Soleimani and al Qaeda senior commander Abu Hafs al-Mauritani at Iran's Zahedan (near the Pakistani and Afghanistan border) during December 2001.<sup>103</sup>

---

<sup>102</sup> Seth Jones, *Al Qaeda in Iran* (Jan. 29, 2012), <https://www.foreignaffairs.com/articles/iran/2012-01-29/al-qaeda-iran>.

<sup>103</sup> Cathy Scott-Clark & Adrian Levy, THE EXILE: THE STUNNING INSIDE OF OSAMA BIN LADEN AND AL-QAEDA IN FLIGHT 93 (2017).

1089. In testimony before the U.S. Senate in February 2003, CIA Director George Tenet said, “we see disturbing signs that al Qaeda has established a presence in both Iran and Iraq.”<sup>104</sup>

1090. Senior al Qaeda members continued to conduct terrorist operations from inside Iran. For example, U.S. intercepted communications from Saif al Adel, then in Mashad, Iran, to al Qaeda assassination teams in Saudi Arabia just before their May 12, 2003 assault on three housing compounds in Riyadh. Al Qaeda leaders in Iran planned and ordered the Riyadh bombing.

1091. CIA Director General Michael Hayden noted that bin Laden understood that Iran was providing safe harbor to al Qaeda. For example – he quoted communications between senior al Qaeda commanders and bin Laden, found on bin Laden’s computer:

“everybody is threatened – as long as he moves – by a missile...There is an idea preferred by some of the brothers to avoid attrition [loss of staff, leaders, and the organization’s old elites] the idea is that some brothers will travel to ‘safe’ areas with their families, just for protection.” The author offers some ideas for safe havens: Sind, Baluchistan, Iran. Two months later bin Laden agrees they should be taking refuge in safer areas.”<sup>105</sup>

1092. After the September 19, 2008 attack on the American embassy in Sana'a, Yemen, which killed 19 people, Ayman al Zawahiri sent a letter to IRGC (which was intercepted) which stated: “Al-Qaeda’s leadership pays tribute to Iran’s generosity, stating that *without its ‘monetary and infrastructure assistance’ it would have not been possible for the group to carry out the terror attacks.*<sup>106</sup> (Emphasis added).

---

<sup>104</sup> David Johnston, *Threats and Responses: Washington; Top U.S. Officials Press Case Linking Iraq to Al Qaeda*, N.Y. TIMES (Feb. 12, 2003), <http://www.nytimes.com/2003/02/12/world/threats-responses-washington-top-us-officials-press-case-linking-iraq-al-qaeda.html>.

<sup>105</sup> Michael W. Hayden, AMERICAN INTELLIGENCE IN THE AGE OF TERROR – PLAYING TO THE EDGE 339-340 (2016).

<sup>106</sup> Con Coughlin, *Iran receives al Qaeda praise for role in terrorist attacks*, THE TELEGRAPH (Nov. 23, 2008), <http://www.telegraph.co.uk/news/worldnews/middleeast/iran/3506544/Iran-receives-al-Qaeda-praise-for-role-in-terrorist-attacks.html>.

1093. Testifying before the Senate Foreign Relations Committee on March 16, 2010, then commander of U.S. Central Command General David Petraeus stated that: al Qaeda “[c]ontinues to use Iran as a key facilitation hub, where facilitators connect al Qaeda’s senior leadership to regional affiliates...”<sup>107</sup>

#### **8. Abu Musab Zarqawi**

1094. In 1999, Abu Musab Zarqawi founded and was the operational leader of Al Tawhid al Jihad (a/k/a Jund al-Islam), an organization with close personal and organizational links to the al-Qaeda network. UBL provided Zarqawi \$200,000 to set up a training camp in Afghanistan near the border with Iran. In 2000, a Jordanian court sentenced Zarqawi in absentia to fifteen years of hard labor for his role in the al Qaeda millennial terror plot targeting Western interests in Jordan.

1095. In early September 2001, Zarqawi met Mohamed Abu Dhess, one of the Tawhid cell operatives in Germany, in Iran. During the meeting, Zarqawi instructed Abu Dhess to commit terrorist attacks against Jewish or Israeli facilities in Germany. Zarqawi’s cell operatives included Mohamed Abu Dhess, Shadi Abdalla, Aschraf Aidagma, and Ismail Shalabi, who were living in Beckum, Germany. The members of the cell planned to use various weapons in order to attack a busy square in a German town or city and another German town in the immediate vicinity of an Israeli or Jewish property with the aim of killing as many people as possible, but were arrested by the German authorities on April 23, 2002.<sup>108</sup>

---

<sup>107</sup> Combatting Terrorism Center at West Point, *CTC Sentinel* (Apr. 2007), [https://ctc.usma.edu/v2/wp-content/uploads/2017/04/CTC-Sentinel\\_Vol10Iss4.pdf](https://ctc.usma.edu/v2/wp-content/uploads/2017/04/CTC-Sentinel_Vol10Iss4.pdf).

<sup>108</sup> U.S. Dep’t of the Treasury, *Treasury Designates Six Al-Qaeda Terrorists* (Sept. 24, 2003), available at <https://www.treasury.gov/press-center/press-releases/Pages/js757.aspx>.

1096. On September 23, 2001, Tawhid (together with Iranian sponsored Ansar al Sunna) took hostages, tortured, and murdered (the majority of which were beheaded) 42 Peshmerga security officers in the Iraqi Kurd border town (on the border with Iran).

1097. In early 2002, Zarqawi escaped from U.S. forces in Afghanistan to Iran with other al Qaeda leaders and operatives.<sup>109</sup> While staying in Iran, Zarqawi operated under the control of the IRGC and the IRGC-QF. Intelligence officials claimed the time Zarqawi spent in Iran was crucial for rebuilding his network before relocating to Iraq to establish the al Qaeda subgroup al Qaeda in Iraq.<sup>110</sup>

1098. Several months later, Zarqawi returned to the Ansar al-Islam camp in northern Iraq, run by his Jund al-Islam/Tawhid lieutenants.<sup>111</sup>

1099. On September 24, 2003, the U.S. Treasury designated Zarqawi and several of his associates as SDGTs, stating that Zarqawi not only has “ties” to Hezbollah, but that plans were in place for his deputies to meet with both Hezbollah and Asbat al Ansar (a Lebanese Sunni terrorist group tied to al Qaeda).<sup>112</sup>

1100. In 2004, Zarqawi changed the name of his group from Al Tawhid to al Qaeda in Iraq.

---

<sup>109</sup> The Washington Institute, *Untangling the Terror Web: Identifying and Counteracting the Phenomenon of Crossover Between Terrorist Groups* (Spring 2004), <https://www.washingtoninstitute.org/uploads/Documents/opeds/4224dcca0249e.pdf>.

<sup>110</sup> United Against Iran, *Alliance Against America: Al Qaeda and Iran*, <https://www.unitedagainstnucleariran.com/node/3295> (last visited Oct. 14, 2017). United Against Iran was founded in 2008 by Ambassador Mark D. Wallace, the late Ambassador Richard Holbrooke, former CIA Director Jim Woolsey and Middle East expert Ambassador Dennis Ross.

<sup>111</sup> SAIS review winter- spring 2004- Untangling the Terror Web: Identifying and Counteracting the Phenomenon of Crossover Between Terrorist Groups-Matthew Levitt, available at <https://www.washingtoninstitute.org/uploads/Documents/opeds/4224dcca0249e.pdf>.

<sup>112</sup> *Supra* n. 108.

1101. US Department of Treasury designated Tawhid al Jihad as an FTO and SDGT on October 15, 2004.<sup>113</sup> OFAC SDN designation was updated on December 1, 2004 to the other known names of al Qaeda in Iraq.<sup>114</sup>

1102. MOIS and IRGC-QF are under the general command of Section 101, also called the Leader's Intelligence and Security office. They cooperate and share intelligence in "exporting the revolution" (which is a euphemism for fomenting violence and destabilizing other regimes, primarily via acts of international terrorism.<sup>115</sup>

1103. Department 15 of MOIS handles liaison responsibilities with foreign terror groups while the IRGC relies on its IRGC-QF for many of the same functions.<sup>116</sup>

1104. On June 10, 2003, American intelligence officials asserted that MOIS and the IRGC-QF are deeply involved in supporting al-Qaeda.<sup>117</sup>

1105. In December 2006, two IRGC-QF agents were arrested in Baghdad, possessing "weapons lists, documents pertaining to shipments of weapons into Iraq, organizational charts, telephone records and maps, among other sensitive intelligence information... [and] information about importing modern specially shaped explosive charges into Iraq. Officials were particularly concerned by the fact the Iranians had information about importing modern, specially shaped explosive charges into Iraq, weapons that have been used in roadside bombs to target U.S.

---

<sup>113</sup> U.S. Dep't of the Treasury, *Recent OFAC Actions* (Oct. 15, 2004), <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20041015.aspx>.

<sup>114</sup> U.S. Dep't of the Treasury, *Recent OFAC Actions* (Dec. 1, 2004), <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20041201.aspx>.

<sup>115</sup> Stratfor, *Iranian Intelligence and Regime Preservation* (June 22, 2010), <https://worldview.stratfor.com/article/special-series-iranian-intelligence-and-regime-preservation>.

<sup>116</sup> William Tucker, *A Reported Shift in Iran's IRGC* (Sept. 29, 2015), <http://inhomelandsecurity.com/a-reported-shift-in-irans-irc/>. In Homeland Security Chief Correspondent William Tucker is a former terror specialist in the United States Army.

<sup>117</sup> U.S. says Iran harbors al Qaeda 'associate,' ' THE WASHINGTON TIMES (June 10, 2003), <http://www.washingtontimes.com/news/2003/jun/10/20030610-125659-6237r/>.

military armored vehicles.”<sup>118</sup> An American intelligence official said these documents “show how the [IRGC-QF]... is working with individuals affiliated with al Qaeda in Iraq and Ansar Al Sunna.”<sup>119</sup> One of the IRGC-QF detainees was probably – according to General Stanley McChrystal – Mohsen Chizari, commander of IRGC-QF’s Operations and Training staff.<sup>120</sup>

1106. “Iranian involvement in Iraq with the Sunni terrorists has been an open secret in military and intelligence circles since the Fallujah uprising in March of 2004. Iranian mines and weapons were funneled to Zarqawi’s terrorists in Fallujah and elsewhere throughout Sunni dominated Anbar province.”<sup>121</sup>

1107. On February 16, 2012, the U.S. Department of Treasury designated MOIS, indicating that it has facilitated al Qaeda operatives in Iran and provided them with documents, identification cards, and passports. The Treasury also stated that MOIS provided money and weapons to al Qaeda in Iraq (a terrorist group designated under E.O. 13224), and negotiated prisoner releases of al Qaeda operatives.<sup>122</sup>

1108. Under Secretary for Terrorism and Financial Intelligence David S. Cohen on July 28, 2011, said that, “[b]y exposing Iran’s secret deal with [al Qaeda], allowing it to funnel funds and operatives through its territory, we are illuminating yet another aspect of Iran’s unmatched support for terrorism. Today’s action [designating the following al Qaeda terrorists and others]

---

<sup>118</sup> *Iraq Expels 2 Iranians Detained by U.S.*, THE WASHINGTON TIMES (Dec. 30, 2006), <http://www.washingtonpost.com/wp-dyn/content/article/2006/12/29/AR2006122901510.html>.

<sup>119</sup> Eli Lake, *Iran’s Secret Plan for Mayhem*, N.Y. SUN (Jan. 3, 2007), <http://www.nysun.com/foreign/irans-secret-plan-for-mayhem/46032/>.

<sup>120</sup> Michael Weiss & Hassan Hassan, *ISIS: INSIDE THE ARMY OF TERROR* 53 (2015).

<sup>121</sup> Bill Roggio, *Iran and Al Qaeda in Iraq*, *FDD’S Long War Journal* (Jan. 6, 2007), available at [http://www.longwarjournal.org/archives/2007/01/iran\\_and\\_alqaeda\\_in.php](http://www.longwarjournal.org/archives/2007/01/iran_and_alqaeda_in.php).

<sup>122</sup> U.S. Dep’t of the Treasury, *Treasury Designates Iranian Ministry of Intelligence and Security for Human Rights Abuses and Support for Terrorism* (Feb. 16, 2012), <https://www.treasury.gov/press-center/press-releases/Pages/tg1424.aspx>.

also seeks to disrupt this key network and deny [al Qaeda's] senior leadership much-needed support...Iran is a critical transit point for funding to support al-Qa'ida's activities in Afghanistan and Pakistan." Among terrorists designated was Ezedin Abdel Aziz Khalil (a/k/a Yasin al-Suri).<sup>123</sup>

1109. Ezedin Abdel Aziz Khalil, a prominent al Qaeda facilitator, who has been operating under a secret agreement between al Qaeda and the Iranian government. The Iranian regime has permitted Khalil to operate within its borders since 2005 and maintain a relationship with him. Khalil moved money and recruits from across the Middle East into Iran, then on to Pakistan for the benefit of al Qaeda senior leaders. He was responsible for moving significant amounts of money via Iran for onward passage to al Qaeda leadership in Iraq and Afghanistan.

1110. Muhsin al-Fadhli, was considered then "an [al Qaeda] leader in the Gulf countries." His 2005 designation states he was "considered an al Qaeda leader in the Gulf" who "provided support to Iraq-based fighters for attacks against" the U.S.-led Coalition. Al-Fadhli was also a "major facilitator" for deceased al Qaeda in Iraq leader Abu Musab al Zarqawi...Al-Fadhli began working with [al Qaeda's] Iran-based facilitation network in 2009 and was later arrested by the Iranians. He was subsequently released by the Iranians in 2011 and went on to assume the leadership of the facilitation network from al Qaeda leader Yasin al-Suri later that year.

1111. Al Qaeda leader Yasin al-Suri along with five other terrorist operatives used his safe harbor in Iran to move funds and recruits from Iran's neighboring Gulf countries to South Asia and elsewhere. Al Suri's network assisted senior al Qaeda operatives in Iraq and Pakistan.

---

<sup>123</sup> U.S. Dep't of Treasury, *Treasury Targets Key Al-Qa'ida Funding and Support Network Using Iran as a Critical Transit Point* (July 28, 2011), <https://www.treasury.gov/press-center/press-releases/Pages/tg1261.aspx>.

1112. On February 5, 2014, the U.S. Treasury Department designated senior al-Qaeda member Jafar al-Uzbeki, part of an al-Qaeda network which operates in Iran “with the knowledge of Iranian authorities.” The Treasury added that this network “uses Iran as a transit point for moving and funding foreign fighters through Turkey to support al Qaeda-affiliated elements inside Syria.”

### **C. IRANIAN SIGNATURE WEAPONS USED IN THE TERRORIST ATTACKS**

#### **1. Explosively Formed Penetrators**

1113. One of Iran’s primary forms of material support and/or resources that facilitated terror attacks against U.S. nationals in Iraq was the financing, manufacturing and deployment of EFPs and IEDs.

1114. IED is shorthand for an Improvised Explosive Device, commonly deployed as a roadside bomb. AAI and the Special Groups consistently sought to attempt to improve IED effectiveness and sophistication.<sup>124</sup>

1115. EFPs, IEDs, and other WMDs were typically smuggled from Iran to Iraq, and the IRGC-QF played a vital role in that process.<sup>125</sup>

1116. Additionally, in Iraq, the IRGC and Hezbollah supplied and trained various Special Groups to deploy EFPs.

1117. EFPs are a particularly effective form of manufactured IED and are sometimes known as a “shaped charge,” usually made with a manufactured concave copper disk and a high explosive packed behind the liner.

---

<sup>124</sup> *Supra* n. 60.

<sup>125</sup> Press Briefing by Multi-National Force-Iraq Deputy Chief of Staff for Strategic Effects Brigadier General Kevin Bergner, *Security Operations in Iraq*, Slide 4.

1118. Once exploded, these EFPs turn into copper slugs capable of penetrating tank armor.

1119. EFPs are manufactured with highly-calibrated machine tools and bear signature imprints showing they were manufactured by Iran.

1120. The EFPs deployed by the IRGC and Hezbollah in Iraq were not truly “improvised” explosive devices but professionally manufactured and specifically designed to target U.S. nationals, including Plaintiffs, and Coalition Forces’ armor, and have far more destructive power than other weapons typically used by terrorists.

1121. These EFPs cannot be made without specific machinery, access to which Iran controls, and without which Special Groups and other terrorist organizations could not obtain or use these munitions.

1122. EFPs constitute “weapons of mass destruction” as that term is defined in 18 U.S.C. § 2332a(2)(A).

1123. In Iraq, EFPs were often triggered by various technologies, including passive infra-red sensors (tripped by the engine heat of passing vehicles) and radio frequency modules (triggering the weapon when high-powered radio waves were generated by Coalition Forces’ jamming devices), ultimately setting off an explosion within the steel casing of the EFP, forcing the copper disk forward, and turning it into a high-velocity molten slug, traveling at over a mile per second, that could pierce the military-grade armor of most U.S. vehicles deployed in Iraq even up to 300 feet away.

1124. Metallurgic analysis by U.S. technicians helped confirm the high-purity copper EFP liners were not generally produced in Iraq.

1125. Differences in the liners indicated the kind of press that was required to fabricate

them—a heavy (hydraulic) press not commonly seen in Iraq.

1126. To produce these weapons, copper sheets are often loaded onto a punch press to yield copper discs. These discs are annealed in a furnace to soften the copper. The discs are then loaded into a large hydraulic press and formed into the disk-like final shape.

1127. The hydraulic press machinery was transported to Iran by Iran's national maritime carrier, Islamic Republic of Iran Shipping Line ("IRISL").

1128. This munitions manufacturing process is critical to the design and concomitant lethality of the weapon and is controlled by Iran.

1129. EFPs are far more sophisticated and destructive than homemade explosive devices such as traditional improvised explosive devices, and they are designed specifically to target vehicles such as armored patrols and supply convoys, though Hezbollah and the Special Groups have deployed them against U.S. and Iraqi civilians as well.

1130. When the explosives inside an EFP detonate, the blast energy inverts the copper disk into a ragged slug weighing several pounds, traveling over a mile per second,<sup>126</sup> and capable of punching through military-grade armor.

1131. One of the ways in which the IRGC provided "militants with the capability to assemble IEDs with EFPs that were specially designed to defeat armored vehicles" included providing them with manufacturing supplies such as copper and steel, as well as machinery—including hydraulic presses used to form copper into the shape of disks used in EFPs.

---

<sup>126</sup> Rick Atkinson, *There was a two-year learning curve . . . and a lot of people died in those two years*, THE WASHINGTON POST (Oct. 1, 2007), [http://www.washingtonpost.com/wp-dyn/content/article/2007/09/30/AR2007093001675\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2007/09/30/AR2007093001675_pf.html).

1132. Numerous U.S. government reports have identified Iran's role in supplying the Special Groups with these weapons and have detailed the devastating effect they have on U.S. military vehicles and service members, including Plaintiffs.

1133. Iran propagated its specialized weapons knowledge up and down its network of terror proxies in Iraq, as the U.S. State Department documented in its 2006 *Country Reports on Terrorism*:

Iran provided guidance and training to select Iraqi Shia political groups, and weapons and training to Shia militant groups to enable anti-Coalition attacks. Iranian government forces have been responsible for at least some of the increasing lethality of anti-Coalition attacks by providing Shia militants with the capability to build IEDs with explosively formed projectiles similar to those developed by Iran and Lebanese Hezbollah. The Iranian Revolutionary Guard was linked to armor-piercing explosives that resulted in the deaths of Coalition Forces. The Revolutionary Guard, along with Lebanese Hezbollah, implemented training programs for Iraqi militants in the construction and use of sophisticated IED technology. *These individuals then passed on this training to additional militants in Iraq.*

(Emphasis added.)

1134. Also in 2006, Brigadier Gen. Michael Barbero, Deputy Chief of Staff for Strategic Operations of the Multi-National Force-Iraq stated: "Iran is definitely a destabilizing force in Iraq. I think it's irrefutable that Iran is responsible for training, funding, and equipping some of these Shi'a extremist groups and also providing advanced IED technology to them, and there's clear evidence of that."

1135. Brigadier Gen. Kevin Bergner commented on Iran funding of Hezbollah operatives in Iraq:

Actions against these Iraqi groups have allowed coalition intelligence officials to piece together the Iranian connection to terrorism in Iraq [...] Iran's [IRGC-QF], a special branch of Iran's Revolutionary Guards, is training, funding, and arming the Iraqi groups. [...] It shows how Iranian operatives are using Lebanese surrogates to create Hezbollah-like capabilities. And it paints a picture of the level of effort in funding and arming extremist groups in Iraq.... The groups operate throughout Iraq. They planned and executed a string of bombings, kidnappings,

sectarian murders and more against Iraqi citizens, Iraqi forces and coalition personnel. They receive arms – including explosively formed penetrators, the deadliest form of improvised explosive device – and funding from Iran. They also have received planning help and orders from Iran.

1136. In May 2007, the Commander of the Multinational Division-Center, U.S. Army Major General Richard Lynch, confirmed that “[m]ost of our casualties have come from improvised explosive devices. That’s still the primary threat to our soldiers—IEDs. And we have an aggressive campaign to counter those IEDs, but they still are taking a toll on our soldiers: 13 killed, 39 soldiers wounded. *What we’re finding is that the technology and the financing and the training of the explosively formed penetrators are coming from Iran.* The EFPs are killing our soldiers, and we can trace that back to Iran.” (Emphasis added.)

1137. That same year, the Deputy Chief of Staff for Intelligence with the MNF-I, U.S. Army Major General Richard Zahner, declared that:

Labels on weapons stocks seized inside and outside Iraq point to Iranian government complicity in arming Shiite militias in Iraq [...] Iran is funneling millions of dollars for military goods into Iraq [...] You’ll find a red label on the C-4 [explosive] printed in English and will tell you the lot number and name of the manufacturer.

Major General Zahner further added:

[T]he control of military-grade explosives in Iran is controlled through the state apparatus and is not committed through rogue elements right there. It is a deliberate decision on the part of elements associated with the Iranian government to affect this type of activities.

1138. According to the U.S. State Department’s 2007 Country Reports on Terrorism:

Despite its pledge to support the stabilization of Iraq, Iranian authorities continued to provide lethal support, including weapons, training, funding, and guidance, to some Iraqi militant groups that target Coalition and Iraqi security forces and Iraqi civilians. In this way, Iranian government forces have been responsible for attacks on Coalition forces. The Islamic Revolutionary Guard Corps (IRGC)-Qods Force, continued to provide Iraqi militants with Iranian-produced advanced rockets, sniper rifles, automatic weapons, mortars that have killed thousands of Coalition and Iraqi Forces, and explosively formed projectiles (EFPs) that have a higher

lethality rate than other types of improvised explosive devices (IEDs), and are specially designed to defeat armored vehicles used by Coalition Forces. The Qods Force, in concert with Lebanese Hezbollah, provided training outside Iraq for Iraqi militants in the construction and use of sophisticated IED technology and other advanced weaponry. These individuals then passed on this training to additional militants inside Iraq, a “train-the-trainer” program. In addition, the Qods Force and Hezbollah have also provided training inside Iraq. In fact, Coalition Forces captured a Lebanese Hezbollah operative in Iraq in 2007.

1139. The U.S. State Department echoed this statement in subsequent reports.

1140. Other U.S. Government reports, such as the Department of Defense’s December 2007 “Measuring Stability and Security in Iraq” quarterly report to Congress, similarly concluded that:

Iranian Islamic Revolutionary Guard Corps - Qods Force (IRGC-QF) efforts to train, equip, and fund Shi'a extremists also continue despite reported assurances to Prime Minister Maliki that Iran will cease lethal aid.

1141. Similarly, in 2011, the U.S. Ambassador to Iraq, James F. Jeffrey, was quoted as saying “[F]resh forensic testing on weapons used in the latest deadly attacks in the country bolsters assertions by U.S. officials that Iran is supporting Iraqi insurgents with new weapons and training. [...] We’re not talking about a smoking pistol. There is no doubt this is Iranian.”

1142. Iran also introduced other weapons into Iraq for the purpose of supporting terrorist attacks on U.S. nationals and coalition personnel, including Plaintiffs. These included 81 mm mortars (the remainder of the region uses 82 mm mortars), repainted 107 mm rockets imported into Iran from China and marked for sale in the open markets, 60 mm canisters filled with Iranian-manufactured mortar rounds; 240 mm rockets, IRAMs, RPG-7s, RPG-29s, and RKG-3 armor penetrating anti-tank grenades deployed by Special Groups in various acts of international terrorism, including the Terrorist Attacks wherein Plaintiffs and/or Plaintiffs’ family members were killed, maimed, or otherwise injured.

## **2. Improvised Rocket Assisted Munitions**

1143. In addition to EFPs, Iran also provided material support for Special Groups by providing them with IRAMs.

1144. Along with EFPs, IRAMs were a signature weapon of terrorists in Iraq that were supplied by the IRGC.

1145. An IRAM is a rocket-fired improvised explosive device made from a large metal canister—such as a propane gas tank—filled with explosives, scrap metal, and ball bearings and propelled by rockets, most commonly 107 mm rockets launched from fixed or mobile sites by remote control. They are designed to cause catastrophic damage and inflict mass casualties.

1146. According to The Joint Improvised Explosive Device Defeat Organization of the U.S. Department of Defense, IRAMs were first introduced by Iran in November 2007 against U.S. personnel in Iraq.

1147. Although Iran's use of IRAMs was publicly disclosed by U.S. officials after their introduction in 2007, systematic identification of specific attacks as IRAM attacks was not publicly disclosed until 2010.

1148. IRAM attacks occurred primarily in Baghdad and in the Shi'a dominated areas in southern Iraq, where Iranian-backed militias primarily operate.

1149. All of the foregoing material support provided to Special Groups, including those Special Groups that perpetrated the Terrorist Attacks that resulted in the death, maiming, or otherwise injuring of Plaintiffs and Plaintiffs' family members, was financed and facilitated in substantial part by material support in the form of funds transfers initiated by Iran through Defendants on behalf of and for the benefit of Hezbollah and other of Iran's Agents and Proxies.

1150. Because Iran is under numerous sanctions issued by other countries, it continues to evade those sanctions by operating clandestinely through Iran and/or its Agents and Proxies, including the IRISL, Mahan Air, and the NIOC.

**D. IRAN EVADES SANCTIONS THROUGH ITS AGENTS/PROXIES**

1151. Iran, its Agents and Proxies, and Defendant Bank Saderat serve as financial and logistical conduits for various terrorist groups, including the Special Groups, and their terrorist activities, specifically including the Terrorist Attacks during which Plaintiffs or Plaintiffs' family members were killed, maimed, or otherwise injured. Defendants knew this fact during the time in which they performed illegal financial transactions for the FTOs responsible for Plaintiffs' deaths or injuries.

1152. In addition to Iran, its Agents and Proxies and the Terrorist Groups, Defendants acted through and with the assistance of other co-conspirators affiliated with Iran. Such co-conspirators include, but are not limited to the Co-Conspirator Banks,<sup>127</sup> as well as the IRISL, the state owned and operated NIOC, and Mahan Air, that serve as financial and logistical conduits for Iran and its Agents and Proxies.

1153. At all relevant times, these Agents and Proxies of Iran acted as Defendants' co-conspirators.

1154. Pursuant to 31 C.F.R. § 560.304, Bank Markazi, Bank Sepah, Bank Melli Iran, and the NIOC constitute the government of Iran.

---

<sup>127</sup> The Co-Conspirator Banks include, but are not limited to, Bank Markazi Jomhouri Islami Iran (a/k/a the "Central Bank of the Islamic Republic of Iran"), Bank Melli Iran, Melli Bank Plc, Bank Mellat, Bank Tejarat, Bank Refah, and Bank Sepah.

1155. Iran obtains weapons and other material support it provides to the Terrorist Groups through its Agents and Proxies that are nothing more than extensions of the Iranian regime.

#### **1. Bank Markazi Jomhouri Islami Iran**

1156. Bank Markazi is the central bank of Iran. The Central Bank of Iran (“CBI”) was established in 1960, and, according to its website, CBI is responsible for the design and implementation of Iran’s monetary and credit policies.<sup>128</sup>

1157. CBI is headquartered at Mirdamad Boulevard, No. 198, Tehran, Iran.

1158. CBI has provided millions of dollars to terrorist organizations via other Iranian-owned and controlled banks. For example, in a press release issued by the U.S. Treasury Department in 2007 regarding the designation of the Iranian-owned Bank Saderat as an SDGT, the U.S. Government noted that:

Bank Saderat, which has approximately 3200 branch offices, has been used by the Government of Iran to channel funds to terrorist organizations, including Hezbollah and European Union-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad. For example, from 2001 to 2006, Bank Saderat transferred \$50 million from the **Central Bank of Iran** through its subsidiary in London to its branch in Beirut for the benefit of Hezbollah fronts in Lebanon that support acts of violence. (Emphasis added.)

1159. According to FinCEN:

The Central Bank of Iran, which regulates Iranian banks, has assisted designated Iranian banks by transferring billions of dollars to these banks in 2011. In mid-2011, the CBI transferred several billion dollars to designated banks, including Saderat, Mellat, [Export Development Bank of Iran] and Melli, through a variety of payment schemes. In making these transfers, the CBI attempted to evade sanctions by minimizing the direct involvement of large international banks with both CBI and designated Iranian banks.

---

<sup>128</sup> Arabic translation, <http://www.alraimedia.com/ar/article/special-reports/2016/06/04/684698/nr/nc> (last visited Oct. 15, 2017).

1160. CBI is an alter-ego and instrumentality of Iran and its Supreme Leader, and it has routinely used Iranian banks like Defendant Bank Saderat or other Iranian Agents and Proxies as conduits for terror financing and weapons proliferation on behalf of the Iranian regime.

## **2. Bank Melli Iran and Mell Bank Plc**

1161. Bank Melli Iran, one of the largest banks in Iran, was established in 1927 by order of the Iranian Parliament.

1162. Following the Iranian Revolution in 1979, all banks in Iran were nationalized, and, as discussed below, even now most are effectively controlled by the Iranian regime.

1163. Bank Melli Iran is headquartered at Ferdowsi Avenue, Tehran, Iran.

1164. Bank Melli Iran maintains a branch office in Germany, located at Holzbrücke 2, 20459 Hamburg, Germany.

1165. Bank Melli Iran is an “agency or instrumentality” of Iran as defined by 28 U.S.C. § 1603(b).

1166. As discussed in detail herein, Bank Melli Iran is dominated and controlled by Iran to such an extent that it rightfully can be considered an organ of the state as defined by 28 U.S.C. § 1603(b)(2).

1167. Mell Bank Plc in London was established in January 2002 as a wholly-owned subsidiary of Bank Melli.

1168. Mell Bank Plc is headquartered at 98a Kensington High Street, London, W8 4SG, United Kingdom.

1169. The Chairman of Bank Melli Iran serves as the Chairman of the Board of Directors of Mell Bank Plc.

1170. Bank Melli Iran appoints all members of the Board of Directors of Mell Bank Plc.

1171. Melli Bank Plc is dominated and controlled by Iran to such an extent that it rightfully can be considered an organ of the state as defined by 28 U.S.C. § 1603(b)(2).

1172. According to the U.S. government, from 2004-2011, Bank Melli Iran and Melli Bank Plc in London transferred approximately \$100 million USD to the IRGC-QF, which trained, armed, and funded terrorist groups that targeted and killed, and maimed American and Iraqi forces and civilians.

1173. According to the U.S. government:

Islamic Revolutionary Guards Corps (IRGC) and IRGC-Qods Force, who channel funds to militant groups that target and kill Coalition and Iraqi forces and innocent Iraqi civilians, have used Bank Melli and other Iranian banks to move funds internationally. Bank Melli used deceptive banking practices to obscure its involvement from the international banking system by requesting that its name be removed from financial transactions when handling financial transactions on behalf of the IRGC.

1174. In October 2007 and throughout the remainder of the Relevant Period, Bank Melli Iran and Melli Bank Plc were each designated as a SDN pursuant to E.O. 13382, and included on OFAC SDN list.<sup>129</sup> The U.S. Treasury Department press release announcing the designation stated:

Bank Melli also provides banking services to the [Iranian Revolutionary Guard Corps] and the Qods Force. Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least \$100 million to the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank Melli has requested that its name be removed from financial transactions.

---

<sup>129</sup> Terrorism and Financial Intelligence Office of Foreign Assets Control, <https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx> (last visited Oct. 15, 2017). “The [OFAC] administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.”

1175. A State Department diplomatic cable from March 2008 noted that:

Bank Melli and the Central Bank of Iran also provide crucial banking services to the Qods Force, the IRGC's terrorist supporting arm that was headed by UNCSR 1747 designee Commander Ghassem Soleimani. Soleimani's Qods Force leads Iranian support for the Taliban, Hezbollah [sic], Hamas [sic] and the Palestinian Islamic Jihad. Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least \$100 million to the Qods Force. Bank Melli use of Deceptive Banking Practices .... When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank Melli has requested that its name be removed from payment instructions for US dollar denominated transactions.

1176. According to the U.S. government, Bank Melli provided banking services to the IRGC-QF to train, arm, and fund terrorist groups that targeted, killed and maimed American and Iraqi forces and civilians.

1177. In addition, during the Relevant Period, Bank Melli Iran helped evade U.S. sanctions on behalf of Mahan Air (an SDGT) and Iran's Ministry of Defense and Armed Forces Logistics.

1178. For example, Bank Melli issued a Letter of Credit ("LC") to Mahan Airlines (an Iranian airline) in August 2004 to help Mahan Airlines illegally acquire aircraft engines subject to the U.S. embargo.

1179. Bank Melli's financial support and assistance to Mahan Airlines is particularly significant because on October 12, 2011, the United States designated Mahan Air as an SDGT for "providing financial, material and technological support to the IRGC-QF. Based in Tehran, Mahan Airlines provides transportation, funds transfers, and personnel travel services to the IRGC-QF."

1180. The Treasury Department explained Mahan Airline's direct involvement with terrorist operations, personnel movements, and logistics the IRGC-QF's behalf:

Mahan Air [has] facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq by bypassing normal security procedures and not including information on flight manifests to eliminate records of the IRGC-QF travel.

Mahan Air crews have facilitated IRGC-QF arms shipments. Funds were also transferred via Mahan Air for the procurement of controlled goods by the IRGC-QF.

In addition to the reasons for which Mahan Air is being designated today, Mahan Air also provides transportation services to Hezbollah, a Lebanon-based designated FTO. Mahan Air has transported personnel, weapons and goods on behalf of Hezbollah and omitted from Mahan Air cargo manifests secret weapons shipments bound for Hezbollah [sic].

1181. Mahan Airlines was also later identified as the conduit to Iran of *thousands* of radio frequency modules recovered by Coalition Forces in Iraq from IEDs and EFPs that were used to target Plaintiffs and Coalition Forces.

1182. In mid-2007, Bank Melli Iran's branch in Hamburg ("Bank Melli-Hamburg") transferred funds on behalf of Iran's DIO.

1183. DIO is an Iranian government-owned defense manufacturer whose name, logo and/or product tracking information was stamped on munitions found in weapons caches that were seized from the Special Groups in Iraq; including large quantities of weapons produced by DIO in 2006 and 2007 (for example, 107-millimeter artillery rockets, as well as rounds and fuses for 60 millimeter and 81 millimeter mortars).

### **3. Bank Mellat**

1184. Bank Mellat provides banking services in support of Iran's WMDs program through the Atomic Energy Organization of Iran and Novin Energy Company.

1185. In 2007, Bank Mellat was designated by the U.S. Treasury Department for providing "banking services in support of Iran's nuclear entities, namely the Atomic Energy Organization of Iran and Novin Energy Company. Both Atomic Energy Organization and Novin Energy have been designated by the United States under E.O. 13382 and by the UN Security

Council under UNCSRs 1737 and 1747.”

1186. During the Relevant Period, Bank Mellat provided financial services and maintained Eurodollar accounts for Atomic Energy Organization and Novin Energy Company, and as part of the Conspiracy, Bank Mellat affirmatively worked to prevent disclosure of its dollar-denominated transactions on behalf of these designated customers.

1187. In June 2006, Bank Mellat was involved in a transfer totaling over \$250 million dollars into a Eurodollar account it held for Novin Energy Company.

1188. As part of the Conspiracy, the CBI effectuated the payment(s) in USD funds to Bank Mellat’s Eurodollar account in London for further credit to the Eurodollar account of Bank Mellat’s client – Novin Energy Company.<sup>130</sup>

1189. In 2007, Bank Sepah facilitated payments in USD funds to Eurodollar accounts at Bank Mellat on behalf of entities associated with Iran’s AIO, a subsidiary of MODAFL that was designated by the United States on June 28, 2005.<sup>131</sup>

1190. The AIO is the Iranian organization responsible for ballistic missile research, development, and production activities and organizations, including the Shahid Hemmat Industries Group and the Shahid Bakeri Industries Group, which were both listed under U.N. Security Council Resolution 1737 and designated by the United States under E.O. 13382.

1191. Bank Mellat was designated by the United States on October 25, 2007 in connection with WMDs proliferation activities, and was included on OFAC’s SDN list. The

---

<sup>130</sup> Novin Energy Company was designated by the U.S. Treasury Department under Exec. Order No. 13382 and by the United Nations Security Council in Resolution 1747.

<sup>131</sup> U.S. Dep’t of the Treasury, *Iran’s Bank Sepah Designated by Treasury Sepah Facilitating Iran’s Weapons Program* (Jan. 9, 2007), <https://www.treasury.gov/press-center/press-releases/Pages/hp219.aspx>. When Bank Sepah was designated by the U.S. in January 2007, the U.S. government noted that “Bank Sepah is AIO’s bank of choice, and since at least 2000, Sepah has provided a variety of critical financial services to Iran’s missile industry, arranging financing and processing dozens of multi-million dollar transactions for AIO and its subordinates...”

designation, *inter alia*, excluded Bank Mellat from accessing the U-turn exemption for Iranian Eurodollar transactions.

1192. In 2002, together with Iran's Bank Tejarat, Bank Mellat merged its London branch to form Persia International Bank Plc in the United Kingdom.

1193. During the Relevant Period, both Defendants HSBC-London and Defendants Barclays maintained Eurodollar accounts for Persia International Bank Plc and served as its "principal bankers" in the Eurodollar market.

1194. "According to court documents, Barclays followed instructions, principally from banks in Cuba, Iran, Libya, Sudan, and Burma, not to mention their names in USD payment messages sent to Barclays' branch in New York and to other financial institutions located in the United States. Barclays routed USD payments through an internal Barclays account to hide the payments' connection to OFAC-sanctioned entities and amended and reformatted the U.S. dollar payment messages to remove information identifying the sanctioned entities. Barclays also deliberately used a less transparent method of payment messages, known as cover payments, as another way of hiding the sanctioned entities identifying information."<sup>132</sup>

1195. "Barclays engaged in this criminal conduct by: (a) following instructions, principally from banks from Cuba, Iran, Libya, Sudan, and Burma not to mention their names in USD payment messages sent to Barclays' branch in New York, New York (the "New York Branch") and to other financial institutions located in the United States; (b) routing USD payments through an internal Barclays sundry account to hide the payments' connection to

---

<sup>132</sup> U.S. Dep't of Justice, *Barclays Bank PLC Agrees to Forfeit \$298 Million in Connection with Violations of the International Emergency Economic Powers Act and the Trading with the Enemy Act* (Aug. 18, 2010), <https://www.justice.gov/opa/pr/barclays-bank-plc-agrees-forfeit-298-million-connection-violations-international-emergency>.

Sanctioned Entities; (c) amending and reformatting USD payment messages to remove information identifying Sanctioned Entities; and (d) deliberately using a less transparent method of payment messages, known as cover payments.

1196. Barclays' conduct, which occurred outside the United States, caused its New York Branch, and other financial institutions located in the United States, to process payments that otherwise should have been held for investigation, rejected, or blocked pursuant to U.S. sanctions regulations administered by OFAC. Additionally, by its conduct, Barclays: (a) prevented its New York Branch and other financial institutions in the United States from filing required Bank Secrecy Act ("BSA") and OFAC-related reports with the U.S. government; (b) caused false information to be recorded in the official records of U.S. financial institutions; and (c) caused U.S. financial institutions not to make records they otherwise would have been required by law to make.

1197. To hide these illegal transactions, Barclays altered and routed payment messages to ensure that payments violating IEEPA, the Trading with the Enemy Act, and OFAC regulations cleared without difficulty though its New York Branch and other U.S. financial institutions. The total value of prohibited transactions for the period of Barclays' review was approximately \$500 million.<sup>133</sup>

#### **4. Bank Sepah**

1198. Bank Sepah is an Iranian government-owned and government-controlled financial institution.

1199. In 2007, the U.S. Treasury Department designated Bank Sepah as a SDN for providing support and services to designated Iranian proliferation firms. The designation was

---

<sup>133</sup> *U.S. v. Barclays Bank, PLC*, Doc. 2-1, Ex. A, Case No. 1:10-cr-00218 (D.D.C. 2010).

effectuated pursuant to E.O. 13382, due to Bank Sepah's WMDs proliferation-related activities.

1200. Bank Sepah International Plc, a wholly-owned subsidiary of Bank Sepah in the United Kingdom, was also designated as a SDN.

1201. According to the U.S. Treasury Department, Bank Sepah was the financial linchpin of Iran's missile procurement network and actively assisted Iran's pursuit of missiles capable of carrying WMDs.

1202. As a result of the designation, Bank Sepah (including Bank Sepah International Plc) was excluded from accessing the U-Turn exemption for Eurodollar transactions.

1203. During the Relevant Period, Defendants HSBC-London provided illegal Eurodollar clearing and settlement services to Bank Sepah.

1204. During the Relevant Period, SCB provided illegal Eurodollar clearing and settlement services for Bank Sepah, as well as facilitating US dollar- denominated Letters of Credit for Bank Sepah. SCB also provided Eurodollar payments and trade-finance services for Bank Saderat and Bank Melli.

1205. As detailed below, Bank Sepah, acting in concert with SCB, illegally financed the acquisition of U.S. goods on behalf of Mahan Air.

1206. For example, in February 2006, Credit Suisse in Zurich paid SCB Dubai almost \$30 million dollars (cleared and settled through the United States) on behalf of Bank Sepah, which had, in turn, financed Mahan Air's acquisition of an Airbus A320-232 and several aircraft engines.<sup>134</sup>

1207. In another case in 2002, Bank Sepah financed (in USD funds) the purchase of

---

<sup>134</sup> Part of the trade-finance transaction was cleared through Standard Chartered's New York branch, and the paperwork indicates that SCB was aware the transaction involved U.S. origin parts prohibited by U.S. sanctions.

U.S. aircraft parts from an Iranian front company—the Malaysian and UK exporter Downtown Trading Ltd. (“Downtown Trading”—on behalf of a MODAFL-controlled entity.

1208. As part of the illegal scheme, once the U.S.-manufactured goods were transported from Malaysia to Iran by Iran Air, Downtown Trading, Malaysia sent documents to its bank, Maybank, Malaysia to collect payment against the LC.

1209. Maybank then presented documents under Bank Sepah’s LC to SCB, Dubai (the Negotiating Bank) for validation and subsequent clearing and settlement of the transaction’s final Eurodollar payment through Citibank, New York.

1210. Thus, Bank Sepah, with the assistance of Maybank and SCB, financed the illegal acquisition of U.S. aircraft parts by MODAFL, and induced Citibank in New York to provide dollar clearing and settlement to consummate the transaction.

1211. As detailed below, Defendants Commerzbank AG, New York branch also provided illegal Eurodollar clearing and settlement services for Bank Sepah members.

## **5. Islamic Republic of Iran Shipping Lines**

1212. Iran’s national maritime carrier, IRISL,<sup>135</sup> is an agent and instrumentality of Iran.

1213. IRISL has a long history of facilitating arms shipments on behalf of the IRGC and the Iranian military, including copper discs that are a key component in EFPs (discussed above) used to kill and maim many of the Plaintiffs herein.

1214. For example, a November 2007 State Department cable noted:

Washington remains concerned about on-going conventional arms transfers from China to Iran, particularly given Iran’s clear policy of providing arms and other support to Iraqi insurgents and terrorist groups like the Taliban and Hezbollah....

---

<sup>135</sup> IRISL is Iran’s national maritime carrier: a global operator of merchant vessels with a worldwide network of subsidiaries, branch offices and agent relationships. It provides a variety of maritime transport services, including bulk, break-bulk, cargo and containerized shipping.

We have specific information that Chinese weapons and components for weapons transferred to Iran are being used against U.S. and Coalition Forces in Iraq, which is a grave U.S. concern.

1215. The diplomatic cable went on to note that an IRISL-flagged vessel was loaded at a Chinese port with multiple containers of cargo bound for delivery at the port of Bandar Abbas, Iran.

1216. The cargo included DIO<sup>136</sup> manufactured ammunition cartridges (7.62 x 39 rounds for AK-47 assault rifles).

1217. DIO is an Iranian government-owned weapons manufacturer controlled by MODAFL.

1218. An April 2008 State Department cable warned of an IRISL shipment of chemical weapons precursors from China aboard the IRISL-leased, Iranian flagged merchant vessel *Iran Teyfouri*.

1219. In September 2008, the U.S. Treasury Department designated IRISL a SDN, stating: "Not only does IRISL facilitate the transport of cargo for U.N. designated proliferators, it also falsifies documents and uses deceptive schemes to shroud its involvement in illicit commerce."

1220. The Treasury Department further noted that:

[i]n order to ensure the successful delivery of military-related goods, IRISL has deliberately misled maritime authorities through the use of deception techniques. These techniques were adopted to conceal the true nature of shipments ultimately destined for MODAFL [Iran's Ministry of Defense and Armed Forces Logistics].

1221. In January 2009, a former Russian merchant ship chartered by IRISL—named the

---

<sup>136</sup> DIO was designated an SDN by the U.S. on March 30, 2007. IRGC Brigadier-General Seyyed Mahdi Farahi was the Managing Director of DIO and has been sanctioned by the European Union since 2008. . . He was later sanctioned by the U.S. on January 17, 2016. See Council Decision 2010/644/CFSP of 25 October 2010 amending Decision 2010/413/CFSP concerning restrictive measures against Iran and repealing Common Position 2007/140/CFSP, <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0644>.

merchant vessel *Monchegorsk* and flying a Cypriot flag—was spotted leaving the Iranian port of Bandar Abbas and heading for the Suez Canal.

1222. Egyptian authorities were alerted by the U.S. Navy, and the merchant vessel *Monchegorsk* was forced into an Egyptian port to be searched. Iran's DIO was later determined to be the shipper of the military-related cargo.

1223. Munitions, believed headed for Gaza, were found hidden in the cargo, including components for mortars and thousands of cases of powder, propellant, and shell casings for 125 mm and 130 mm guns.

1224. In October 2009, U.S. troops boarded a German-owned freighter, the merchant vessel *Hansa India*, in the Gulf of Suez and found eight containers full of ammunition that were headed to Syria from Iran.

1225. The vessel carried seven containers of small arms ammunition (including 12 million bullet casings), as well as one container containing copper discs of the type used in EFPs to kill and maim Coalition Forces and U.S. nationals, including Plaintiffs.

1226. The acronym “IRISL” was painted in large block letters on the exterior side walls of each shipping container, and the barrels of munition parts discovered inside the containers were marked with the inscription “SAEZMANE SANAYE DEFA,” a common transliteration from Farsi to English of the name for Iran's DIO.

1227. The merchant vessel *Hansa India* was registered to the Hamburg-based shipping company Leonhardt & Blumberg, but had been under charter to IRISL for several years.

1228. In November 2009, the Government of Israel intercepted an IRISL-flagged ship, the merchant vessel *Francop*, headed for Beirut, Lebanon and then Latakia, Syria. The vessel was loaded with munitions crates that were either stamped “IRISL” or included documentation

marked with the IRGC-QF logo.

1229. The munitions found onboard included over two thousand 107 mm “Katyusha” rockets, more than six hundred 122 mm “Grad 20” rockets, and also various rocket fuses, mortar shells, rifle cartridges, fragment grenades and 7.62 mm bullets.

1230. The merchant vessel *Francop*, owned by the Cypriot shipping company UFS, was carrying shipping containers clearly marked IRISL.

1231. United Nations Security Council Resolution 1929, adopted on June 9, 2010, froze certain assets of IRISL and called on the international community to cease providing financial and insurance services to both the IRGC and IRISL.

1232. In addition, a July 2010 European Union sanctions implementing regulation confirmed that IRISL conducted deceptive business practices in order to access USD funds.

1233. Specifically, European Union Council Implementation Regulation Number 668/2010 stated that “IRISL subsidiaries have used US dollar-denominated bank accounts registered under cover- names in Europe and the Middle East to facilitate routine fund transfers.”

1234. Similarly, the June 2011 indictment of IRISL in New York stated:

In many aspects of global commerce, including the international maritime industry, contracts and payments are denominated in USDs. Such USD transactions are primarily executed, or “cleared,” through correspondent banks in the United States. The USD clearing operations for many large U.S. financial institutions are processed through correspondent bank accounts domiciled in New York County.

In order to deceive and bypass these OFAC filters, SDNs designated under OFAC’s non-proliferation of weapons of mass destruction program must falsify, or cause to be falsified, the originator and/or beneficiary information in wire transfers. In other words, by omitting or falsifying data regarding their roles as the true originators or beneficiaries, SDNs are able to send and receive wire transfers that would otherwise be blocked by U.S. financial institutions. Through the fraudulent use of a web of subsidiary entities and front companies, IRISL and the other defendants were able to deceive U.S. financial institutions and maintain their access to the U.S. financial system.

1235. Because the DIO, as discussed *infra*, was one of MODAFL's three main weapons systems manufacturers, it was required to use IRISL for most of its illicit shipments of military-related raw-materials, parts, and finished products for, and from, foreign suppliers, Iranian arms dealers, and terrorist organizations.

1236. Iran's DIO was listed as an entity of concern for military procurement activities in an early warning document distributed by the German government to industry in July 2005.

1237. The DIO was also designated by the United Nations in 2006 for its involvement in Iran's WMDs program.

1238. During 2006 and 2007, weapons caches seized by Coalition Forces from the Special Groups in Iraq contained large quantities of weapons produced by Iran; including many 107 mm artillery rockets with closely clustered DIO lot numbers and production dates between 2005 and 2007, as well as rounds and fuses for 60 millimeter and 81 millimeter mortars with DIO lot markings and 2006 production dates.

1239. According to the U.S. State Department, the DIO was the owner of a Eurodollar account that was maintained by Bank Melli Iran's branch in Hamburg; and this bank account was used to send and receive USD funds transfer transactions for the benefit of the DIO.

1240. IRISL facilitated shipments of military cargo to FTOs and Special Groups, including those responsible for carrying out the Terrorist Attacks that killed, maimed, and/or injured Plaintiffs or Plaintiffs' family members.

1241. IRISL *did*, in fact, facilitate shipments of military cargo to Hezbollah.

1242. However, IRISL was not Iran's only means of obtaining weapons to pass on to Special Groups charged by Iran with committing acts of international terrorism, including the Terrorist Attacks carried out against Plaintiffs and/or Plaintiffs' family members.

## 6. National Iranian Oil Company

1243. The NIOC, owned and overseen by the Government of Iran through its Ministry of Petroleum, is responsible for the exploration, production, refining, and export of oil and petroleum products in Iran.

1244. NIOC is headquartered at Hafez Crossing, Taleghani Avenue, Tehran, Iran, P.O. Box 1863 and 2501.

1245. NIOC is an “agency or instrumentality” of the Government of Iran as defined by 28 U.S.C. § 1603(b). Pursuant to 31 C.F.R. § 560.304, the NIOC is the government of Iran.<sup>137</sup>

1246. In 2008, the Treasury Department identified NIOC (and other Iranian agencies) as “centrally involved in the sale of Iranian oil, as entities that are owned or controlled by the [Government of Iran].”

1247. At all relevant times, the NIOC was controlled by Iran through the IRGC.

1248. During the Relevant Period, the NIOC not only was under IRGC control, but it also served a critical function in supporting the IRGC’s activities.

1249. The Iranian Helicopter Aviation Company, Ahwaz Pipe Mill Co., and Kala Naft<sup>138</sup> are all subsidiaries of the NIOC.

1250. As early as February 1998, Kala Naft was identified by the UK government “as having procured goods and/or technology for weapons of mass destruction programs.”

---

<sup>137</sup> Office of Foreign Asset Control, *Sanctions Search List*, <https://sanctionssearch.ofac.treas.gov/Details.aspx?id=5608> (last visited Oct. 15, 2017).

<sup>138</sup> U.S. Dep’t of the Treasury, *Recent OFAC Actions* (June 16, 2010), <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20100616.aspx>.

1251. Kala Naft was also publicly identified as a NIOC subsidiary in a 2003 Commerce Department action that further stated that Kala Naft was a recipient of illegally exported U.S. origin oilfield equipment from the U.S.

1252. Pursuant to E.O. 13382, the U.S. Government designated NIOC as an SDN.

1253. The U.S. Government has identified NIOC as an agent or affiliate of the IRGC.

1254. In September 2012, the U.S. Treasury Department handed its report to Congress regarding its determination that NIOC is an agent or affiliate of the IRGC. The report provided that:

Recently, the IRGC has been coordinating a campaign to sell Iranian oil in an effort to evade international sanctions, specifically those imposed by the European Union that prohibit the import, shipping, and purchase of Iranian oil, which went into full effect on July 1, 2012. NIOC, which is owned by the Government of Iran through the Ministry of Petroleum, is responsible for the exploration, production, refining, and export of oil and petroleum products in Iran.

Under the current Iranian regime, the IRGC's influence has grown within National Iranian Oil Co. For example, on August 3, 2011, Iran's parliament approved the appointment of Rostam Qasemi, a Brigadier General in the IRGC, as Minister of Petroleum. Prior to his appointment, Qasemi was the commander of Khatam Al-Anbia, a construction and development wing of the IRGC that generates income and funds operations for the IRGC. Even in his new role as Minister of Petroleum, Qasemi has publicly stated his allegiance to the IRGC.

1255. Under the Iran Threat Reduction and Syria Human Rights Act of 2012 ("ITRSRHA"), the U.S. government determined that that NIOC is an agent or affiliate of the IRGC under section 104(c)(2)(E)(i) of the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 and section 302 of ITRSHRA. As part of that 2012 certification, NIOC was formally determined to be part of the Government of Iran.

1256. In addition, the ITRSHRA provided that:

It is the sense of Congress that the National Iranian Oil Company and the National Iranian Tanker Company are not only owned and controlled by the Government

of Iran but that those companies provide significant support to Iran's Revolutionary Guard Corps and its affiliates.<sup>139</sup>

1257. NIOC used its oil and natural gas revenues to launder money for the IRGC, often using Defendants CBI for this purpose.

1258. In 2009, West Point's Combating Terrorism Center published a report on the role of NIOC, particularly in the Maysan province in Iraq (Southeast border between Iran and Iraq), and its role in studying U.S. troops movements:

The establishment of a new U.S. and Iraqi [FOB] on the Iranian border has resulted in three waves of attacks in an area that was formerly devoid of incidents .... The incident occurred in the same district as the February 2007 EFP attack on a British aircraft at a Buzurgan dirt airstrip, itself a reaction by Special Groups to UK long-range patrolling of the Iranian border. This part of the border is increasingly the scene of U.S. and Iranian countermoves to support their proxies and patrol the frontier; Iranian intelligence gathering takes place using National Iranian Oil Company helicopters and border guards, while U.S.-Iraqi helicopter-borne joint patrols provide moral and material support to isolated Iraqi border posts and local communities.

1259. Thus, NIOC served a critical function in funding and supporting the IRGC's activities in Iraq, including the use of Special Groups and other terror groups such as AAI.

1260. NIOC also obtained letters of credit from Western banks, including SCB, to provide financing and credit to the IRGC.<sup>140</sup>

## 7. Mahan Air

1261. On October 12, 2011, the United States designated the Iranian commercial airline Mahan Air as a SDGT for "providing financial, material and technological support to the [IRGC-

---

<sup>139</sup> See Iran Threat Reduction and Syria Human Rights Act of 2012, available at [https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwi0wp2YsvXWAhVD5CYKHY-uAlAQFggmMAA&url=https%3A%2F%2Fwww.treasury.gov%2Fresource-center%2Fsanctions%2FDocuments%2Fhr\\_1905\\_pl\\_112\\_158.pdf&usg=AOvVaw01qJaNyum9pYm\\_9V6KKz\\_\\_](https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwi0wp2YsvXWAhVD5CYKHY-uAlAQFggmMAA&url=https%3A%2F%2Fwww.treasury.gov%2Fresource-center%2Fsanctions%2FDocuments%2Fhr_1905_pl_112_158.pdf&usg=AOvVaw01qJaNyum9pYm_9V6KKz__).

<sup>140</sup> The Superseding Indictment filed in *U.S. v. Zarab*, Case No. 1:15-cr-00867 (S.D.N.Y.) demonstrates that, as late as 2013, NIOC continued to illegally launder USDs through U.S. financial institutions, <https://www.justice.gov/opa/file/834146/download>.

QF].”

1262. According to the U.S. government, Mahan Air (1) “facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq;” (2) “facilitated IRGC-QF arms shipments;” and (3) “transported personnel, weapons and goods on behalf of Hezbollah. [sic].” (Brackets in original).

1263. The Treasury Department explained Mahan Air’s direct involvement with terrorist operations, personnel movements and logistics on behalf of the IRGC-QF:

Mahan Air also facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq by bypassing normal security procedures and not including information on flight manifests to eliminate records of the IRGC-QF travel.

Mahan Air crews have facilitated IRGC-QF arms shipments. Funds were also transferred via Mahan Air for the procurement of controlled goods by the IRGCQF.

In addition to the reasons for which Mahan Air is being designated today, Mahan Air also provides transportation services to Hezbollah [sic], a Lebanon-based designated Foreign Terrorist Organization. Mahan Air has transported personnel, weapons and goods on behalf of Hezbollah [sic] and omitted from Mahan Air cargo manifests secret weapons shipments bound for Hezbollah [sic].

1264. Under Secretary of Commerce Eric L. Hirschhorn described this supply chain as “egregious conduct by... foreign companies and individuals who have endangered the lives of U.S. and coalition forces in Iraq.”

1265. Mahan Air was also later identified as the conduit to Iran of thousands of radio frequency modules recovered by Coalition Forces in Iraq from IEDs that were used to target U.S. nationals, including Plaintiffs, and Coalition Forces.<sup>141</sup>

1266. Coalition Forces recovered these modules in Iraq from IED devices that were

---

<sup>141</sup> *United States v. Larjani*, Case No. 1:10-cr-00174-EGS (D.D.C. 2010), <https://www.justice.gov/opa/file/837996/download>.

used to target U.S. nationals, including Plaintiffs, and Coalition Forces.

1267. The modules had encryption capabilities and a particularly long range that allowed Special Groups operatives to operate them across significant distances.

1268. In 2008, Mahan Air transported the IED components from Singapore and Thailand to Tehran, Iran.

1269. In short, at the direction of Iran, Mahan Air transported weapons, personnel, and technology into Iraq on behalf of the IRGC-QF and Hezbollah, and did, in fact, transport modules used to control and activate IEDs and EFPs deployed against Coalition Forces in Iraq.

1270. Mahan Air, in its supporting albeit crucial role of exporting terrorism, and the materials and instruments thereof, for Iran, is an agent and instrumentality of Iran.

1271. Due to the role played by Mahan Air, in connection with Defendants' participation in the Conspiracy, Iran was able to effectuate global jihadism and commit acts of terrorism much more effectively and conveniently during the Relevant Period, including the time in which the Terrorist Attacks were committed.

#### **8. Khatam al-Anbiya Construction Company & The Headquarters for the Restoration of Holy Shrines**

1272. Khatam al-Anbiya Construction Company (a/k/a Khatam al-Anbiya Construction Headquarters, Qaraghah-e Sazandegi-ye Khatam al-Anbiya, or "Seal of the Prophets," hereinafter referred to as "KAA"), is a large Iranian corporation, controlled by the IRGC, and serves to help the IRGC fund its operations.

1273. KAA is an agent/instrumentality of Iran as it is designated as an IRGC entity, and thus, is owned and controlled by the government of Iran.

1274. Iran clandestinely and financially supports terrorist groups through Iran's Agents and/or Proxies, including, but not limited to KAA, an IRGC-QF front, as well as its agents and subsidiaries.

1275. IRGC Commander-in-Chief, Major General Mohammad Ali Jafari, serves as KAA's council chairman.

1276. KAA functions as the IRGC's engineering and logistical arm, conducting a range of civil engineering activities, such as road and dam construction, the manufacturing of pipelines to transport water, oil, gas (within and outside Iran's borders), mining operations, agriculture, and telecommunications.

1277. On October 25, 2007, KAA was designated by the U.S. Treasury Department under E.O. 13382 for extensively assisting IRGC to gain financial support for IRGC activities.

1278. Treasury designated nine IRGC-affiliated entities, including KAA, and five IRGC-affiliated individuals as derivative designations of the IRGC.

1279. On June 23, 2008, the European Union also designated IRGC-affiliated companies, including KAA, for their support to Iranian ballistic missile and nuclear programs.

1280. On June 9, 2010, the U.N. Security Council designated KAA in the 1929 Resolution for its involvement with Iranian military and nuclear activities.<sup>142</sup>

1281. On February 10, 2010, The U.S. Department of the Treasury took further action to implement then-existing U.S. sanctions against the IRGC by designating an individual and four companies affiliated with the IRGC pursuant to Executive Order (E.O.) 13382, which freezes the assets of designated proliferators of WMDs and their supporters. This action focused in

---

<sup>142</sup> Security Council Imposes Additional Sanctions on Iran, Voting 12 in Favour to 2 Against, with 1 Abstention (June 9, 2010), <https://www.un.org/press/en/2010/sc9948.doc.htm>.

particular on KAA, considered an arm of the IRGC designated pursuant to E.O. 13382 in 2007.

At the time, Treasury stated:

Today's designations include IRGC General Rostam Qasemi, who is also the commander of KAA, the engineering arm of the IRGC that serves to help the IRGC generate income and fund its operations. KAA is owned or controlled by the IRGC and is involved in the construction of streets, highways, tunnels, water conveyance projects, agricultural restoration projects, and pipelines. Treasury also today designated four companies that are owned or controlled by, or that act on behalf of, KAA.

1282. As the IRGC consolidates control over broad swaths of the Iranian economy, displacing ordinary Iranian businessmen in favor of a select group of insiders, it is hiding behind companies like KAA and its affiliates to maintain vital ties to the outside world," said Under Secretary for Terrorism and Financial Intelligence Stuart Levey. "Today's action exposing KAA subsidiaries will help firms worldwide avoid business that ultimately benefits the IRGC and its dangerous activities."

1283. In 2011, the British and Japanese governments both listed KAA as an entity of potential concern due to its involvement in the proliferation of WMDs, missiles, and biological, chemical, and nuclear weapons.

1284. Despite the appearance of KAA being involved in civilian projects, the company mainly deals in non-civilian, military related work. A senior IRGC official told the Iranian press that "70% of KAA's work is non-civilian projects." <sup>143</sup>

1285. KAA has been involved in construction projects for Iran's ballistic missile and nuclear programs, KAA subsidiaries were heavily involved in the construction of the uranium enrichment site at Qom/Fordow, and it has been listed as an entity of the IRGC.<sup>144</sup>

---

<sup>143</sup> Andrew Higgins, *A Feared Force Roils Business in Iran*, WSJ, Oct. 14, 2006.

1286. KAA serves to help the IRGC disguise its funding and operations, including IRGC-QF terror activities.

1287. Companies that are owned or controlled by KAA, or that act on its behalf, and directly support its efforts include: Fater Engineering Institute, Imensazen Consultant Engineers Institute (ICEI), Makin Institute, and Rahab Institute.

1288. KAA has undertaken some infrastructure development projects in Iraq, Syria, and Lebanon, extending its services as a soft power tool for Iran.

1289. KAA was operating on the ground in Iraq during the entire Relevant Period.

1290. No later than October 2006, western media outlets were reporting that KAA was involved in hidden and unlawful economic activities beyond the borders of Iran.

1291. On May 7, 2008, Mohammad Reza Pourzeyai, then KAA deputy head announced that KAA had built a railway line connecting Iraq's Basra and Iran's Khorramshar.

1292. KAA also performed due diligence and planned a project for building a water pipeline from the Iraqi border to the middle of Syria, a distance of approximately 256 kilometers, and also designed a project for building an oil pipeline from Iran's Abadan refinery to Basra, Iraq.

1293. KAA also undertook efforts to renovate the Mosul Dam in Iraq. KAA's work on Dam projects around the globe is a known conduit through which the IRGC moves its operatives into foreign countries.

1294. On December 13, 2011, then commander of KAA, Abu al-Qassem Mozaffari, confirmed that KAA operates in Iraq, Syria, and Lebanon.

---

<sup>144</sup> United Nations Security Council, *Security Council Imposes Additional Sanctions on Iran, Voting 12 in Favour to 2 Against, with 1 Abstention* (June 9, 2010), <https://www.un.org/press/en/2010/sc9948.doc.htm>.

1295. A critical IRGC agent, subsidiary, and Iranian-proxy is the Headquarters for the Restoration of Holy Shrines (“HRHS”).

1296. HRHS was established in 2003, purportedly to renovate the Shiite shrines in Iran and in Iraq. In order to do so, HRHS enlisted the assistance of KAA.

1297. According to its charter, as listed on its website, HRHS was authorized by the Islamic regime to, among other things, renovate Shiite shrines in Iraq and to coordinate between the Iranian regime and Iraqi government organizations and NGOs.

1298. HRHS does not hide its links to the IRGC-QF; a provincial official in the HRHS told Iranian media the organization is affiliated with the IRGC-QF.

1299. The commander of the IRGC-QF, Qassem Soleimani, and the supreme leader’s representative to the IRGC-QF both sit on HRHS’s Board of Trustees. The four other board members include HRHS head Hassan Pelarak and three senior clerics who are members of the Supreme Leader’s office. The Supreme Leader and his top general responsible for external operations thus control HRHS.

1300. Hassan Pelarak is a former mining executive and former IRGC commander, and, according to Iranian media, has served in the IRGC-QF.

1301. All HRHS heads have served as IRGC-QF officers. Pelarak’s predecessors Hassan Danaifar, who is now Iran’s ambassador to Iraq, and Mansour Haghighatpour, who is now a former parliamentarian, have been IRGC-QF officers. In 2008, Soleimani touted Danaifar’s IRGC-QF credentials in a famous message passed along to, General David Patraeus, commander of U.S. forces in Iraq.

1302. It is no coincidence that Qassem Soleimani sits on HRHS's Board of Trustees and that organization's Directors have been IRGC-QF officers; the unit uses the infrastructure of the HRHS to funnel weapons, manpower, money, equipment, and supplies into Iraq.

1303. HRHS publishes on its website that it renovates Shiite shrines in Najaf, Karbala, Kadhimiya, Samarra, and other places.

1304. HRHS claims to have spent millions of dollars on more than 200 projects in Iraq and further plans to develop projects valued at approximately \$1.6 billion.

1305. HRHS also claims that its finances are charitable donations from citizens, as well as government, private, and quasi-government entities.<sup>145</sup>

1306. HRHS embraces and supports the Special Groups. The direct link between HRHS and the Special Groups is concretely reflected on its official website of the HRHS Samarra office.<sup>146</sup>

1307. HRHS considers the Special Groups to be "Defenders of the Shiite Holy Shrines in Iraq," as stated on websites controlled by the IRGC-QF.<sup>147</sup>

1308. HRHS is nothing more than a front for the IRGC-QF, whose mission is to support the Iranian-backed terror groups in Iraq, disrupt the stability of free and democratic Iraq, and expand Iranian influence in the country.

1309. HRHS and KAA worked closely together in Iraq.

---

<sup>145</sup> Amir Toumaj, *Qods Force front group develops shrine in Iraq*, THE LONG WAR JOURNAL, Sept. 23, 2016.

<sup>146</sup> See <http://setadsamarra.ir/> (last visited Sept. 13, 2017) (translation available).

<sup>147</sup> *Introduction with the Brigades of the Defenders of the Shiite Holy Shrines operating in Iraq* (Jan. 12, 2015), <http://oweis.ir> (Arabic translation available); *Where and How Volunteers for Fighting ISIS are Trained?"* *Tasnim (Iran)* (June 23, 2014), <http://www.tasnimnews.com/fa/news/> (Farsi web address and translation available).

1310. HRHS worked in cooperation with the IRGC-QF-affiliated KAA to perform construction work on the Zahra Shrine in Najaf, Iraq. This project involved the HRHS subsidiary, Kowsar Engineering.

1311. Under the guise of serving the faithful, KAA and HRHS act as a pipeline for the IRGC-QF, whose mission is to support the Iranian-backed Iraqi network and expand Iranian influence in the country.

1312. KAA and HRHS, much like its IRGC affiliates, work closely with the well-known FTO, Hezbollah. This relationship was highlighted following the assassination of IRGC-QF senior commander Hassan Shateri (a/k/a Hesam Khoshnevis) in February 2013.

1313. Shateri was deployed to Lebanon by KAA to lead its Lebanese branch, while at the same time Shateri was serving as senior IRGC-QF commander.

1314. Shateri's role in the Lebanese branch of KAA extended far beyond construction projects into extensive terror activities. On August 3, 2010, the U.S. Department of Treasury designated Hassan Shateri "for providing technical support to Hezbollah's reconstruction efforts in Lebanon and to the expansion of the terrorist group's private communications network. Khoshnevis also operates as President Ahmadinejad's personal representative in Lebanon."

1315. Shateri arrived in Lebanon after the Lebanon War of 2006 in order to rehabilitate Hezbollah's operational infrastructure damaged during the conflict and to replace Hezbollah's lost arsenal and rebuild its missile sites close to the demarcation line with Israel. Shateri served as a Special Representative of the IRGC, sitting on Hezbollah's Central Command where he helped shape Hezbollah's policies with advice from Secretary-General Hassan Nasrallah.

1316. Prior to working in Lebanon, Shateri operated in Afghanistan, where his mission was to renovate regions that were damaged during fighting with Coalition Forces in Afghanistan.<sup>148</sup>

1317. Between his services in Afghanistan and Lebanon, Shateri was operating in Iraq.<sup>149</sup>

1318. Though his detailed activities in Iraq were concealed, the Supreme Leader's Representative to the IRGC-QF, Ali Shirazi, mentioned Shateri's time there, saying he was dispatched to Iraq as part of his extensive service for the Islamic Revolution.<sup>150</sup>

1319. In or around February 2013, after Shateri's assassination, Hezbollah published details that showed that KAA functioned as a cover for IRGC-QF insurgent activities.

1320. From 2002 through 2007, Defendants Bank Melli and Bank Mellat sent and received payments totaling nearly USD \$100 million for KAA.

1321. As of July 2007, both Banks Melli and Mellat were headed by UNCSR 1737 designee and former IRGC Commander Rahim Safavi.

1322. Defendants Bank Melli and Bank Mellat also provided material support to KAA and its subsidiaries by handling their letters of credit. These letters of credit are primarily used to finance KAA's purchase of equipment and services from overseas suppliers.

---

<sup>148</sup> Holding the fourth anniversary of Shahid Beheshti Sharif + Pictures, available at <https://www.tasnimnews.com/fa/news/> (Farsi web address and translation available).

<sup>149</sup> Dexter Filkins, *The Shadow Commander*, THE NEW YORKER (Sept. 30, 2013), <https://www.newyorker.com/magazine/2013/09/30/the-shadow-commander>.

<sup>150</sup> Will Fulton, *The Assassination of Iranian Quds Force General Hassan Shateri in Syria* (Feb. 28, 2013), [https://www.criticalthreats.org/analysis/the-assassination-of-iranian-quds-force-general-hassan-shateri-in-syria#\\_edn77e9a9b2d5a1d9d20e5cb794c934c9632](https://www.criticalthreats.org/analysis/the-assassination-of-iranian-quds-force-general-hassan-shateri-in-syria#_edn77e9a9b2d5a1d9d20e5cb794c934c9632).

1323. KAA subsidiaries serviced by Bank Melli and/or Bank Mellat include the designated entities Ghorb Nooh, Sepasad, Sahel Consultant Engineers, and Gharargah Sazandegi Ghaem.

1324. Defendants illegally processed USD transfers on behalf or at the request of Banks Melli and Mellat. Without Defendants assisting in the facilitation of such USD transfers, Banks Melli and Mellat would not have been able to provide such USDs to or for the benefit of KAA and HRHS.

1325. KAA and HRHS' activities in Iraq from 2003 until the present provided the perfect vehicle through which Iran smuggled and disguised raw materials, currency, weapons, and munitions used by the Special Groups and other terrorist organizations to effectuate Iran's campaign of terror in Iraq.

#### **E. IRAN'S NEED FOR U.S. DOLLARS**

1326. Some FTOs, including those who perpetrated the Terrorist Attacks, raise significant funds outside of the United States for conduct directed and targeted at the United States.

1327. International terrorism campaigns require significant funding for direct operational support of specific acts of terrorism, as well as funding for broader organizational development.

1328. One of the ways terrorist organizations raise funds is through the support and sponsorship by governments and states. But these funds have no value unless the terrorist organization can move the funds through its organization and among agents.

1329. The global financial system, especially the financial systems of economically stable countries, provides terrorist organizations their principal means of moving their funds.<sup>151</sup>

1330. For these reasons, the USD is the currency of choice, indeed necessary, in financing terrorist operations in Iraq and other countries.

1331. Iran was desperately dependent on access to the USD funds it maintained in the Eurodollar market, and the income its petrodollar deposits generated.

1332. Moreover, reliably consistent access to, and the ability to facilitate trade in, the Eurodollar market has been critical to the capacity of Iran to fund terrorist groups such as Hezbollah and to fuel its other terrorism and weapons proliferation activities through the IRGC.

1333. Without the vital assistance of Defendants, Iran and its Agents and Proxies could not have conducted their terror campaign to the same extent and magnitude, and Iran would have been severely hampered in its terror financing WMD proliferation activities.

1334. During the last fifteen years, while Western governments increased pressure against terrorism financing after al Qaeda's September 11, 2001 attacks on the U.S., Iran intensified its efforts to access the U.S. financial system and U.S. export-controlled technologies, spare parts, and raw materials while simultaneously evading U.S. sanctions, export restrictions, and other laws and regulations intended to circumscribe its access to these capabilities and resources.

1335. The importance to Iran of funding Hezbollah, the IRGC, and the Terrorist Groups became even more acute after the 2003 U.S. invasion of Iraq.

---

<sup>151</sup> U.S. Dep't of the Treasury, *Financial Action Task Force Report on Terrorist Financing* (Feb. 29, 2008), [https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/terrorist-financing\\_022008.pdf](https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/terrorist-financing_022008.pdf).

1336. After the invasion, Iran directed Hezbollah to create Unit 3800 and began devoting greater financial resources to gain influence in Iraq, inflict casualties on U.S. nationals in Iraq, and intensify its quest for WMDs.

1337. After the United States designated Iran as a State Sponsor of Terrorism in 1984 and imposed economic actions limiting its access to the U.S. financial system, Iran and its Agents and Proxies, in concert with entities such as and including Defendants, began developing schemes to circumvent those sanctions and continue the movement of its funds through the U.S. financial system. These schemes evolved into the Conspiracy complained of herein.

1338. Iran was able to rely upon the willingness of Defendants to substantially and materially assist Iran in violation of various sanctions and laws, despite the coordinated and ever-intensifying efforts of the United States, the European Union, and the United Nations after 9/11 to isolate Iran and restrict Iran's capacity to fund terrorism and obtain WMDs.

1339. The money laundered by Defendants as part of the Conspiracy was used to fund the Terrorist Attacks which killed or injured Plaintiffs.

1340. Iran's goals could not have been accomplished without USD funds, access to the Eurodollar market, and the agreement of Western financial institutions, such as Defendants, to shield Iran's unlawful Eurodollar and trade-finance activities from detection.

#### **F. THE U.S. SANCTIONS ON IRAN**

1341. Since Iran's 1984 designation as a "State Sponsor of Terror," the United States has attempted to constrain and deter Iran's sponsorship and perpetuation of terrorist activities by imposing a wide variety of trade and economic sanctions intended to reduce the flow of financial resources, especially USD-denominated assets, for Iran's support of such activities, and thereby prevent the very Terrorist Attacks that killed or injured Plaintiffs or their family members.

1342. Some of the sanctions were created and implemented pursuant to the IEEPA and the Iran Sanctions Act of 1996.

1343. The IEEPA, 50 U.S.C. §§ 1701-1706, authorized the President of the United States to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States when the President declared a national emergency with respect to that threat. It authorizes Executive action to safeguard U.S. national security interests by freezing or blocking assets of belligerent foreign governments or certain foreign nationals abroad. It is a crime to willfully violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under IEEPA.

#### **1. Sanctions Under the International Emergency Economic Powers Act**

1344. On November 14, 1979, ten days after the start of the Iran hostage crisis in which Iranian revolutionaries seized the United States embassy in Tehran and took most embassy personnel as hostages, President Carter exercised his powers under the IEEPA and blocked all property and interests in property of the Government of Iran subject to the jurisdiction of the United States.<sup>152</sup> Presidents Clinton and Bush also issued Executive Orders under the IEEPA directly targeting Iran and its support of international terrorism, which remain active IEEPA emergencies.

##### **a. Executive Order 12957**

1345. On March 15, 1995, President Clinton issued Executive Order No. 12957, finding the actions and policies of the Government of Iran constitute an unusual and extraordinary threat

---

<sup>152</sup> Exec. Order No. 12170, 44 Fed. Reg. 65,729 (Nov. 14, 1979); *see* Transactions Involving Property in Which Iran or Iranian Entities Have an Interest, 31 C.F.R. § 535.201.

to the national security, foreign policy, and economy of the United States, and declaring a national emergency to deal with that threat.

1346. In response, President Clinton followed this with E.O. No. 12959, issued on May 6, 1995, which imposed comprehensive trade and financial sanctions on Iran. These sanctions prohibited, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, to Iran or the Government of Iran of any goods, technology, or services from the United States or by U.S. persons, wherever located. This included persons in a third country with knowledge or reason to know that such goods, technology, or services are intended specifically for supply, transshipment, or re-exportation, directly or indirectly, to Iran or the Government of Iran.

1347. On August 19, 1997, President Clinton issued E.O. No. 13059, consolidating and clarifying E.O. Nos. 12957 and 12959. The Executive Orders authorized the U.S. Secretary of the Treasury to promulgate rules and regulations necessary to carry out the Executive Orders. Pursuant to this authority, the Secretary of the Treasury promulgated the Iranian Transactions Regulations, 31 C.F.R. Part 560.

1348. Except for certain exempt transactions, the ITRs prohibited U.S. depository institutions from servicing Iranian accounts and directly crediting or debiting Iranian accounts.

1349. One such exemption would be transactions for which a validated export license had been obtained from OFAC. The ITRs also prohibit transactions that evade or avoid, have the purpose of evading or avoiding, or attempt to evade or avoid the restrictions imposed under the ITRs. The ITRs were in effect at all times relevant to the conduct described herein.

1350. Iran's access to the international financial system enables the Iranian regime to facilitate its support for terrorism and proliferation. The Iranian regime disguises its involvement

in these illicit activities using a wide array of deceptive techniques, specifically designed to avoid suspicion and evade detection by responsible financial institutions and companies. Iran also is finding ways to adapt to existing sanctions, including by turning to non-designated Iranian banks to handle illicit transactions.

1351. As a result, U.S. depository institutions are no longer allowed to process U-turn transfers to or from Iran, or for the direct or indirect benefit of persons in Iran or the Government of Iran. The prohibition on U-turns applies not only to state-owned Iranian banks and the CBI, but also to privately-owned Iranian banks, Iranian companies, and the settlement of third-country trade transactions that involve Iran.<sup>153</sup>

b. Executive Order 13224

1352. On September 23, 2001, President Bush issued Executive Order 13224 in response to the terrorist attacks on September 11, 2001. The Order was intended to disrupt the financial support network for terrorists and terrorist organizations by authorizing the U.S. Treasury, in consultation with other U.S. government agencies, to designate and block the assets of foreign individuals and entities that commit, or pose a significant risk of committing, acts of terrorism. The Order authorizes the U.S. Treasury to block the assets of individuals and entities that provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under the Order, as well as their subsidiaries, front organizations, agents, and associates.

1353. Pursuant to Executive Order 13224, the IRGC-QF, Hezbollah, and Bank Saderat were designated a SDGT.

---

<sup>153</sup> U.S. Dep't of the Treasury, *Treasury's Further Financial Restrictions on Iran* (Nov. 6 2008), <http://iipdigital.usembassy.gov/st/english/article/2008/11/20081107105758eaifas0.1254084.html#ixzz4bWeXpDMY>.

1354. SDGTs are entities and individuals whom OFAC finds have committed or pose a significant risk of committing acts of terrorism, or whom OFAC finds provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under OFAC Counter Terrorism Sanctions programs, as well as such persons' subsidiaries, front organizations, agents, or associates. This designation effectively prohibits transactions between the designated group and U.S. citizens and freezes group assets under U.S. jurisdiction.

1355. On June 25, 1996, a truck bomb decimated a building at the Khobar Towers complex in Saudi Arabia that was used to house American military personnel, killing 19 Americans and wounding another 372 people. Shortly thereafter, it was established that terrorist operatives responsible for the bombing were trained and equipped by the IRGC.

1356. That same year (1996), Congress responded to the IRGC-funded attack on the Khobar Towers in Saudi Arabia by passing the now-named Iran Sanctions Act.<sup>154</sup> Congress found:

- a) The efforts of the Government of Iran to acquire weapons of mass destruction and the means to deliver them and its support of acts of international terrorism endanger the national security and foreign policy interests of the United States and those countries with which the United States shares common strategic and foreign policy objectives.
- b) The objective of preventing the proliferation of weapons of mass destruction and acts of international terrorism through existing multilateral and bilateral initiatives requires additional efforts to deny Iran the financial means to sustain its nuclear, chemical, biological, and missile weapons programs.
- c) The Government of Iran uses its diplomatic facilities and quasi-governmental institutions outside of Iran to promote acts of international terrorism and assist its nuclear, chemical, biological, and missile weapons programs.

---

<sup>154</sup> The original enactment was called the Iran-Libya Sanctions Act. Congress amended the enactment in 2006 to remove its applicability to Libya. *See*, 50 U.S.C. § 1701.

1357. The Iran Sanctions Act mandated sanctions against two types of transactions: (1) foreign investment in the development of the petroleum sector of Iran; and (2) exportation of sensitive weaponry, both WMDs and advanced conventional ordnance, to Iran.

1358. The 2010 Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 extended sanctions on Iran.

## **2. Iran Evades Sanctions**

1359. Congress and successive Administrations have enacted several laws and executive orders that imposed sanctions on countries and firms that sell WMDs technology and military equipment to Iran. Despite these efforts, Iran continued to evade sanctions.

1360. In order to thwart U.S. sanctions efforts, Iran cultivated close relationships with foreign arms suppliers, including Russia, China, and North Korea.

1361. For years, U.S. law enforcement officials, customs agents and intelligence services worked to thwart Iranian efforts to circumvent U.S. economic sanctions and arms embargos.

1362. A few brief examples illustrate the larger U.S. government effort:

- a) On June 11, 2001, Saeed Homayouni and Yew Leng Fung, officials of Multicore, Inc., pled guilty in the U.S. in connection with the firm's purchase of commercial and military aircraft parts and missile components for export to Iran.
- b) In March 2008, the U.S. led efforts to pass U.N. Security Council Resolution 1803 that called upon all member states "to exercise vigilance over the activities of financial institutions in their territories with all banks domiciled in Iran, in particular with Bank Melli and Bank Saderat, and their branches and subsidiaries abroad" and "to inspect the cargoes to and from Iran, of aircraft and vessels, at their airports and seaports, owned or operated by Iran Air Cargo and Islamic Republic of Iran Shipping Line, provided there are reasonable grounds to believe that the aircraft or vessel is transporting [prohibited] goods..."
- c) On September 17, 2008, the DOJ unsealed a criminal indictment against 16 foreign-based defendants related to Mayrow General Trading Company, for their involvement in providing weapons of mass destruction-related, military, and dual-

use items to Iran, specifically components found in IEDs in Iraq that caused deaths and injuries to U.S. military personnel.

- d) On December 11, 2009, at the request of the U.S. government, the Thai government detained a Russian aircraft containing a cargo of weapons from North Korea destined for Iran.
- e) On June 23, 2010, the U.S. DOJ charged an Iranian company and citizen, as well as Opto Electronics PTE, Ltd., a Singapore company and others with, *inter alia*, violations of the Arms Export Control Act (22 U.S.C. § 2778) for facilitating the unlawful transfer of long range radio frequency modules used in IEDs targeting Coalition Forces and U.S. nationals in Iraq. The modules were flown to Iran by Mahan Air.

1363. In addition, both the U.S. Treasury Department and Commerce Department have blacklisted a long list of Iranian front companies, shell companies and middlemen the U.S. has determined to be complicit in Iran's sanctions evasion efforts.

1364. In an attempt to enforce these sanctions, the United States relied heavily on its financial system as a means of identifying prohibited conduct and preventing resources from getting into the hands of Iranian-backed terrorist groups.

### **3. The U.S. Financial System as a Frontline Defense**

1365. To ensure that U.S. Financial institutions which process international wire transfers in the Eurodollar market do not assist Iran in its support of international terrorism and weapons proliferation or facilitate other prohibited transactions, U.S. financial institutions are required to use sophisticated computer systems to monitor and screen all wire transfer activities.

1366. Banks that process most of the world's Eurodollar payments and foreign exchange transactions depend on these automated systems to prevent Iran and other sanctioned entities (as well as terrorists, money launderers, and other criminals) from gaining access to the United States banking system. In this way, U.S. financial institutions are supposed to be the first line of defense to prevent Iran from accessing the U.S. financial system to fund or otherwise engage in terrorism and other prohibited conduct.

1367. As part of its vital national security mission, the U.S. Treasury Department issues subpoenas to the Society for Worldwide Interbank Financial Telecommunication (“SWIFT”) – a Belgium-based company operated by the Society for Worldwide Interbank Telecommunications. SWIFT maintains U.S. offices and operates a worldwide messaging system (“SWIFT-NET”) used to transmit financial transaction in the Eurodollar market, among other financial markets, in a standardized message format. These subpoenas seek information on suspected international terrorists or their networks. Under the terms of the subpoenas, the U.S. Government may only review information as part of specific terrorism investigations.

1368. Based on information that identifies an individual or entity, the U.S. Government is able to conduct targeted searches against the limited subset of records provided by SWIFT in order to trace financial transactions related to suspected terrorist activity.

1369. SWIFT information greatly enhances the ability to map out terrorist networks, often filling in missing links in an investigative chain. The U.S. Government acts on this information – and, for counter-terrorism purposes only, shares leads generated by the Terrorist Finance Tracking Program with relevant governments’ counter-terrorism authorities – to target and disrupt the activities of terrorists and their supporters.

1370. SWIFT information and the intelligence gathered from the reporting of financial transactions allows authorities to indict illegal or improper funds, develop a better understanding of the financial networks that facilitates terrorism, and ultimately prevents terrorism from occurring by limiting the funds available to terrorists.

## **VII. THE CONSPIRACY**

1371. Defendants entered into a conspiracy with Iran and its Agents and Proxies, agencies and instrumentalities, including the IRGC, the IRGC-QF, Hezbollah, al Qaeda, the Terrorist Groups, Bank Melli Iran, the CBI, Bank Mellat, Bank Tejarat, Bank Refah and Bank

Sepah, the IRISL, the NIOC, Mahan Air, and other front companies, alter egos, and entities owned, controlled by or affiliated with the foregoing, by and through which Defendants knowingly agreed to transfer hundreds of billions of dollars and conduct billions of dollars in illicit trade-finance transactions, as well as provide expert advice, all in violation of U.S. and international laws and sanctions, by altering, falsifying, or omitting information from bank-to-bank payment orders sent on SWIFT-NET operated by the SWIFT that involved Iran or Iranian parties and that serve as financial and logistical conduits for the IRGC and its terrorist activities.

1372. Throughout the Relevant Period, and even before, Iran had the goal of sponsoring terrorism to kill and maim U.S. nationals as a means to achieve its foreign policies.

1373. Iran continued through the Relevant Period to spend USDs on its terrorism campaign.

1374. Those dollars were used to pay terrorists directly and to pay for material support and resources to those terrorists to commit acts of terrorism against U.S. nationals.

1375. To obtain the USDs necessary to fund this massive terrorism campaign, Iran conspired with Defendants to evade and overcome the laws and sanctions that were put in place with the singular goal of stopping Iran from sponsoring and spreading terrorism, especially in the Middle East, including against U.S. nationals.

1376. During the Relevant Period, Iran obtained hundreds of billions of USDs in funds and resources with the help, active participation, and involvement of Defendants.

1377. During the Relevant Period, Defendants made billions of dollars in profits.

1378. During this time, Defendants knew, or were deliberately indifferent to the fact, the resources and assistance they were providing would be used to materially support terrorist attacks that were part of Iran's extensive terrorism campaign.

1379. If Iran had simply stopped sponsoring terrorism and killing U.S. nationals, the sanctions against it would have ended.

1380. The U.S. and the rest of the world were not opposed to Iran's participation in trade finance transactions or trading its oil for USD—provided that Iran stopped sponsoring terrorism.

1381. The laws and sanctions, of course, directly affected Iran's ability to engage in trade finance transactions and trade oil for USD, hence the need for the covert and illegal involvement of Defendants in a scheme to evade the sanctions.

1382. Put simply, sponsoring terrorism (including in Iraq beginning before 2003) was the single driver underlying the object of the conspiracy. Stated differently, the international terrorism Iran sponsored furthered the overall conspiracy by driving the need for the Defendant Bank's active and extensive involvement in it.

1383. Defendants willingly participated—despite knowing the civil, criminal, and reputational risks—because of the enormous fees the conspiracy generated for them.

1384. The objective of the Conspiracy was to defeat the sanctions put in place by the United States, the European Union, and the United Nations to stop Iran from sponsoring acts of international terrorism and proliferating weapons of mass destruction.

1385. In order to achieve the objective of the Conspiracy, Defendants knowingly:

- a) Concealed Iran's dollar-denominated financial activities and transactions from detection, scrutiny, or monitoring by U.S. regulators, law enforcement, and/or depository institutions;
- b) Prevented U.S. intelligence and law enforcement agencies from interdicting the illicit payments and financing transactions, and stopping the flow of billions of dollars to Special Designated Nationals, some of which are FTOs, SDTs, or SDGTs;

- c) Provided expert advice and financial services to Iran and its Agencies and Proxies.

1386. Defendants' conduct in furtherance of the Conspiracy:

- a) Facilitated illicit transactions totaling at least \$50 million USD for the benefit of Hezbollah;
- b) Facilitated illicit transactions totaling at least \$100 million in USD funds for the direct benefit of the IRGC and billions in USD funds for the benefit of the NIOC, then controlled by the IRGC;
- c) Facilitated at least hundreds of illicit transactions totaling more than \$60 million on behalf of IRISL, including over 150 "stripped" transactions after IRISL was designated an SDN;
- d) Facilitated tens of millions of dollars in illicit transactions on behalf of MODAFL, the IRGC, Mahan Air, and other instrumentalities of Iranian state-sponsored terror to further numerous violations of the U.S. trade embargo against Iran, conceal Iran's efforts to evade U.S. sanctions, and enable Iran's acquisition from the United States of goods and technologies prohibited by U.S. law to be sold or transferred to Iran, including components of IEDs deployed against Coalition Forces in Iraq;
- e) Enabled Iran and its Agents and Proxies to authorize, plan, and commit acts of international terrorism as defined in 18 U.S.C. § 2331(1), including (1) providing material support to terrorists prohibited by 18 U.S.C. § 2339A; (2) providing material support or resources to designated FTOs prohibited by 18 U.S.C. § 2339B; and (3) engaging in financial transactions with a government of a country designated under 6(j) of the Export Administration Act prohibited by 18 U.S.C. § 2332d; and
- f) Enabled Iran and its Agents and Proxies to authorize, plan, and commit acts of international terrorism including homicides, attempted homicides, or conspiracies to commit homicide prohibited by 18 U.S.C. § 2332(a)-(c); bombings using destructive devices prohibited by 18 U.S.C. § 2332a; bombings and attempted bombings prohibited by 18 U.S.C. § 2332f; engaging in terrorist activity under 8 U.S.C. § 1189(a)(3)(B)(iii)-(iv); and/or engaging in terrorism under 22 U.S.C. § 2656f.

1387. Without Iran's ability to illegally clear dollars through the U.S. financial system,

Defendants knew the economic sanctions would effectively prevent Iran and its Agents and Proxies from sponsoring acts of international terrorism.

1388. As a reasonably foreseeable consequence of the Conspiracy, Iran and its Agents and Proxies, including the Terrorist Groups, would commit acts of terrorism against U.S. nationals, including Plaintiffs.

1389. Absent the collusion and conspiratorial conduct of Defendants, Iran and its Agents and Proxies could not have successfully hidden the volume of USD clearing and trade-finance transactions they succeeded in illegally clearing through the United States in USD.

1390. Because of the criminal collusion and conspiratorial conduct of Defendants, Iran, and Iran's Agents and Proxies, the United States intelligence agencies, as well as counterterrorism and law enforcement entities, were unable to interdict illegal funds transfers and thereby prevent terrorists from accessing USD funds.

1391. The banks knew the economic sanctions were put in place to cripple the Iranian economy, which would force Iran's leaders to cease their sponsorship of terrorism, which could after a period of time result in the sanctions being lifted. Despite having knowledge of the purpose of the sanctions, the banks processed billions of USD in wire transfers and trade finance for the benefit of Iran in direct violation of the sanctions.

1392. The Conspiracy identified in this Complaint first began in the years immediately after Iran was designated a State Sponsor of Terrorism. As a result of that designation, Iran developed various ways to circumvent U.S. economic sanctions levied against the regime and to facilitate the free movement of USD that Iran obtained without detection by the U.S. government in order to pursue foreseeably illicit objections, such as the objectives outlined above.<sup>155</sup>

---

<sup>155</sup> Defendants willfully circumvented the sanctions screening, anti-money laundering, and combatting the financing of terrorism requirements of OFAC, SWIFT-Brussels, Clearing House Interbank Payment System (“CHIPS-NY”), CLS Bank International, Federal Reserve Bank of New York, and the Fedwire Funds Service (“Fedwire”). CHIPS is a Systemically Important Financial Market Utility for the U.S. financial system and the primary provider of clearing and settlement services in USD funds for Eurodollar transactions. CLS Bank is a

1393. To further those objectives, Iran enlisted several Iranian state-owned banks, as well as Defendant Bank Saderat and various international financial institutions, including Defendants in this action, which agreed to alter, falsify, or omit information from payment order messages that involved Iran or Iranian parties, in particular several Iranian banks (including Defendant Bank Saderat), for the express purpose of concealing Iran's financial transactions from detection, scrutiny, or monitoring by U.S. regulators, law enforcement, and/or depository institutions.

1394. Through the Conspiracy, and with the assistance of Defendants, Iran provided substantial and material support to its Agents and Proxies, who targeted U.S. nationals in Iraq.

1395. Without the material and substantial assistance knowingly provided by Defendants to Iran, Iran could not have concealed and disguised the nature, location, source, and origin of the material support it provided to its Agents and Proxies.

1396. At the time they provided material support to Iran in the form of USD, expert advice, and financial services, it was reasonably foreseeable and Defendants knew the material support would be used in preparation for and in carrying out acts of international terrorism against U.S. nationals and others, including civilians, in Iraq.

1397. The Conspiracy fueled acts of international terrorism targeted at U.S. nationals, specifically including the Terrorist Attacks, and caused Plaintiffs' injuries and the deaths of their loved ones.

1398. Because of the size and scope of Iran's efforts to murder Americans in Iraq—and subvert the U.S.-sponsored and freely elected Iraqi government—Iran required access to

---

Systemically Important Financial Market Utility for the U.S. financial system and the primary provider of clearing and settlement services for foreign exchange transactions in the Eurodollar market, and FRBNY is one of the twelve U.S. Federal Reserve Banks and the central bank lender-of- last-resort for the Eurodollar market (via Fedwire).

hundreds of millions of USD that it could only reliably and effectively transfer through the global financial system with the illicit assistance of Defendants.

1399. The Conspiracy foreseeably enabled Iran and its Agents and Proxies to provide Terrorist Groups with a combination of funding, weapons, munitions, intelligence, logistics, sanctuary, and training, who killed, injured, or maimed Plaintiffs and/or their family members in Iraq during the Relevant Period.

1400. Each co-conspirator knew Iran was a designated State Sponsor of Terrorism at the time it entered into the Conspiracy, as well as throughout the course of the Conspiracy. Each co-conspirator knew it was illegal to facilitate the transfer of funds to Iran and its Agents and Proxies, specifically including the Terrorist Groups, without providing sufficient data to allow the transactions to be adequately detected by OFAC. Each Defendant laundered funds for Iran while concealing their actions from U.S. regulatory authorities and law enforcement. Each co-conspirator assisted in preventing U.S. regulatory authorities and law enforcement from interdicting the contraband fund and preventing Iran from gaining access to hundreds of billions of USD. Iran subsequently used those funds to perpetrate the terrorist acts that resulted in the deaths and injuries of thousands of U.S. nationals, and others.

1401. Each Defendant knew, or was willfully indifferent to, the foreseeable, probable, and inevitable consequences of their funneling of billions of USD to Iran—the violence and death caused by acts of international terrorism.

1402. Without the active participation of Defendants in the Conspiracy, Iran would not have been able to transfer such a large volume of funds to its Agents and Proxies, and thus, would not have been able to perpetrate the Terrorist Attacks.

1403. The connection between money, in particular USD, and Iran and its Agents and Proxies was illustrated in a 2009 diplomatic cable which stated: IRGC and the IRGC-QF, who channel funds to militant groups that target and kill Coalition and Iraqi forces and innocent Iraqi civilians, have used Bank Melli and other Iranian banks to move funds internationally. Bank Melli used deceptive banking practices to obscure its involvement from the international banking system by requesting that its name be removed from financial transactions when handling financial transactions on behalf of the IRGC.

1404. Iran enlisted the assistance of its state-owned banks and Defendants in concealing its financial transactions from detection, scrutiny, and/or monitoring by U.S. regulators, law enforcement, and/or depository institutions. In effect, Defendants not only laundered billions of USD for Iran, some of which was used to fund the Terrorist Attacks, they also effectively concealed the source and use of these funds from regulators, intelligence, and law enforcement who, but for this concealment, could have moved to stop the funds and prevent their reaching the hands of the Terrorist Groups who committed the Terrorist Attacks.

1405. At the time of the improper wire transfers at issue here, Defendants knew the FTOs with which they were doing business were designated terrorists organizations (as that term is defined at 18 U.S.C. § 2339B(g)(6)), and that those FTOs had engaged and were engaging in terrorist activity (as that term is defined in section 212(a)(3)(B) of the Immigration and Nationality Act).

1406. The illicit, clandestine funding, financial services, and material support intentionally provided by Defendants, as well as their conspiracies to conceal such funding from law enforcement, was foreseeably and inevitably utilized by the Terrorist Groups to perpetrate

the Terrorist Attacks. Thus, Defendants' actions were a proximate cause of the deaths and injuries of Plaintiffs.

**A. PERPETRATING THE CONSPIRACY**

1407. Defendants conspired with Iran and its Agents and Proxies to, among other things, launder money.

1408. Money laundering generally refers to financial transactions in which criminals, including terrorist organizations, attempt to disguise the proceeds, sources or nature of their illicit activities. Money laundering facilitates a broad range of serious underlying criminal offenses and ultimately threatens the integrity of the financial system.<sup>156</sup>

1409. In short, Iranian terrorist cells (organization proxies) perpetrated acts of international terrorism (i.e., bombing, kidnappings, extortion, and murder). The IRGC and its proxy Hezbollah provided training, weapons, safe harbor, cash, intelligence and otherwise command and control of the Special Groups perpetrating the attacks. Defendants provided access to the United States financial system and to USD, which were necessary to perpetrate those acts of international terrorism.

1410. Iran enlisted the assistance of Defendants in concealing its financial transactions from detection, scrutiny, and/or monitoring by U.S. regulators, law enforcement, and/or depository institutions.

1411. As detailed above, Defendants not only laundered billions of USD for Iran and its Agents and Proxies, but they also concealed the parties involved from regulators, intelligence, and law enforcement who, but for this concealment, could have moved to stop the funds and

---

<sup>156</sup> U.S. Dep't of the Treasury, *Financial Action Task Force Report on Terrorist Financing* (Feb. 29, 2008), [https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/terrorist-financing\\_022008.pdf](https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/terrorist-financing_022008.pdf).

prevent such funds from reaching the hands of Iran and its Agents and Proxies, including the Terrorist Groups who perpetrated the Terrorist Attacks.

1412. However, through the active participation of all Defendants in the Conspiracy, these laundered funds did reach Iran and the Terrorist Groups, and were used by them to perpetrate the Terrorist Attacks which killed or injured Plaintiffs.

1413. To effectuate the Conspiracy and to avoid being caught, Defendants, with the knowledge, assistance, and agreement of Iran, (1) stripped wire transfer information; (2) made non-transparent cover payments; and (3) utilized U-turn exemptions from certain wire transfers in their concerted effort to hide information which would identify the fact funds being wired were originating from and/or being transferred to Iran and/or its Agents and Proxies. Monies exchanged in these wire transfers were used to fund Iran's Agents and Proxies, specifically including the Terrorist Groups, and to perpetrate the Terrorist Attacks which killed or injured Plaintiffs.

1414. Through their intentional conduct, Defendants specific aims and objectives were to profit by keeping U.S. depository institutions, law enforcement, and counter-terrorism agencies blind to Iran's and/or its Agents' and Proxies' movement of USD through the U.S. and international financial systems.

1415. Defendants did, in fact, profit from their scheme; but in doing so, they proximately caused U.S. nationals, including Plaintiffs and their family members, to suffer death, catastrophic injury, and severe physical and emotional pain and suffering.

1416. Each time Defendants performed a transaction requested by Iran through Defendant Bank Saderat or other Iranian Agents and Proxies, Defendants knew or should have known Defendant Bank Saderat or other Iranian Agents and Proxies were acting as an agent for

the Terrorist Groups that perpetrated the Terrorist Attacks that resulted in the deaths, maiming, or serious injury to Plaintiffs. Such a result was not only possible, it was foreseeable by any responsible person or entity.

1417. Utilizing these correspondent bank accounts in the Southern District of New York to send money to Terrorist Groups violates the statutes under which Plaintiffs are claiming relief herein.

### **1. Stripping Wire Transfer Information**

1418. Stripping refers to the practice of removing wire transfer information that would identify the origination or source of a financial transfer. By stripping away information that identifies a prohibited originator (*e.g.*, Iran), financial institutions can push prohibited transfers past the U.S. financial system screening software that would otherwise reject or freeze them for further inquiry. Stripping effectively conceals that the parties involved are sanctioned entities.

1419. As detailed above, OFAC enforces sanctions designed to block countries and groups from accessing the U.S. banking system. With minor exceptions, U.S. citizens and institutions are prohibited from conducting financial transactions with them. To ensure they comply with these prohibitions, U.S. banks and financial institutions use sophisticated computer systems to monitor and screen all wire transfer activities. Banks in the United States that process most of the world's USD payments depend on these automated systems to prevent sanctioned entities, terrorists, money launderers, and other criminals from gaining access to the U.S. banking system. Thus, the financial institutions are the first line of defense in protecting the U.S. financial system.

1420. In the spring of 2006, the New York District Attorney's Office discovered evidence of fraud in the processing of international wire transfers by at least some Defendants on behalf of their client-Iranian banks. The Iranian banks maintained correspondent accounts with

Defendants. These correspondent accounts constitute the relationships between banks that allow funds to move all over the world, and are essential to international commerce. Defendants illegally maintained correspondent accounts on behalf of sanctioned Iranian banks.

1421. The initial evidence of criminal conduct consisted of information concerning individuals with close ties to Iran located in the United States. These individuals received wire transfers from Bank Melli and other Iranian banks. However, the incoming wire transfers to the U.S. accounts of these individuals did not contain any reference to the Iranian banks or individuals that originated the funds transfers. Instead, the payment messages made it appear the wire transfers originated from Defendants.

1422. This stripping was a systemic, across-the-board operation. To further execute the Conspiracy, Defendants removed, and/or instructed Defendant Bank Saderat or other Iranian Agents and Proxies to remove, any Iranian wire payment references from the wire transfer and then manually re-entered the payment information so the transfer would be processed without detection by government officials.

## **2. Non-Transparent Cover Payments**

1423. International wire payments generally are executed via the secured communications services provided by SWIFT, and the communications underlying the actual payments are commonly referred to as SWIFT messages. When a bank customer sends an international wire payment, the de facto standard to execute such a payment is the MT 103 SWIFT message (also called a serial payment, or a serial MT 103 payment). When a financial institution sends a bank-to-bank credit transfer, the de facto standard is the MT 202 SWIFT message. The crucial difference, during the Relevant Period, was that MT 202 payments typically did not require the bank to identify the originating party to the transactions, and banks typically did not include that information in MT 202 messages. A cover payment typically

involves both types of messages: an MT 103 message identifying all parties to the transaction is sent from the originating bank to the beneficiary, but the funds are transferred through the United States via a MT 202 message that lacks that detail.

1424. Instead of using MT 103 payment messages for transactions involving the Sanctioned Entities, which would have revealed the identity of the ordering customer and beneficiary, Defendants used MT 202 cover payment messages for these bank-to-bank credit transfers, which did not.

1425. As a result, U.S. financial institutions were unable to detect when payments were made to or from a Sanctioned Entity.

### **3. U-Turns**

1426. While the ITRs promulgated for Iran prohibited USD transactions, they contained a specific exemption for USD transactions that did not directly credit or debit a U.S. financial institution. This exemption is commonly known as the U-turn exemption.

1427. The U-turn exemption permitted banks to process Iranian USD transactions that began and ended with a non-U.S. financial institution, but were cleared through a U.S. correspondent bank. In relevant part, the ITRs provided that U.S. banks were authorized to process transfers of funds to or from Iran, or for the direct or indirect benefit of persons in Iran or the Government of Iran, if the transfer . . . is by order of a foreign bank which is not an Iranian entity from its own account in a domestic bank . . . to an account held by a domestic bank . . . for a [second] foreign bank which is not an Iranian entity. 31 C.F.R. § 560.516(a)(1). That is, a USD transaction to or for the benefit of Iran could be routed through the United States as long as a non-U.S. offshore bank originated the transaction and the transaction terminated with a non-U.S. offshore bank. These U-turn transactions were only permissible where no U.S. person or entity

had direct contact with the Iranian bank or customer and were otherwise permissible (e.g., the transactions were not on behalf of an SDN).<sup>157</sup>

1428. By 2008 it was clear that this system of wire transfer checks had been abused, and that U.S. foreign policy and national security could be compromised by permitting U-turns to continue. In November 2008, the U.S. Treasury Department revoked authorization for U-turn transactions because it suspected Iran of using its banks – including the CBI/Markazi, Bank Saderat, and Bank Melli – to finance its nuclear weapons and missile programs. The U.S. also suspected that Iran was using its banks to finance terrorist groups, including Hezbollah, Hamas, and the Palestinian Islamic Jihad, and engaging in deceptive conduct to hide its involvement in various other prohibited transactions, such as assisting OFAC-sanctioned weapons dealers.<sup>158</sup>

1429. Specifically, OFAC revoked the U-turn exemption on November 10, 2008. In revoking the exception, OFAC explained:

Iran's access to the international financial system enables the Iranian regime to facilitate its support for terrorism and proliferation. The Iranian regime disguises its involvement in these illicit activities through the use of a wide array of deceptive techniques, specifically designed to avoid suspicion and evade detection by responsible financial institutions and companies. Iran also is finding ways to adapt to existing sanctions, including by turning to non-designated Iranian banks to handle illicit transactions.

As a result of today's action, U.S. depository institutions are no longer allowed to process U-turn transfers to or from Iran, or for the direct or indirect benefit of persons in Iran or the Government of Iran. The prohibition on U-turns applies not only to state-owned Iranian banks and the Central Bank of Iran, but also to privately-owned Iranian banks, Iranian companies, and the settlement of third-country trade transactions that involve Iran.<sup>159</sup>

---

<sup>157</sup> *United States v. Crédit Agricole Corporate and Investment Bank S.A.* – Appendix A Factual Statement, Case No. 1:15-cr-00137-CKK, (D.D.C. Oct. 20, 2015).

<sup>158</sup> New York State Department of Financial Services, *In the Matter of Standard Chartered Bank, New York Branch*. Order Pursuant to Banking Law § 39, ¶17 (Oct. 12, 2012).

<sup>159</sup> *Supra* n. 153.

#### 4. Trade Finance

1430. Another form of facilitation perhaps even more lucrative for the banks than dollar clearing, is trade finance. According to the DPAs, Defendants provided trade finance to Iran and Iran's trading partners. Trade finance serves two primary functions.

1431. First, trade finance is used to decrease the risk of buying and selling goods in the international market. This is accomplished when a trusted bank acts as the intermediary between two untrusting trading partners. In such cases, the bank acting as intermediary will hold the intended proceeds until it confirms the underlying transaction has been completed, (i.e. the oil has arrived at the intended destination) at which time the bank will transfer the money to the seller. A well-known example of a company providing this type of trade finance is the company known as PayPal. PayPal became an instant hit as an online payment service that allows individuals and businesses to transfer funds electronically, in such a way that it minimizes the risk to both the buyer and seller.

1432. The second function of trade finance is, as the name implies, to provide financing for the buyer or the seller, or both. Often the seller will want to receive the proceeds from the sale before delivery has occurred. The bank will lend the seller money based on the expectation the sale will be completed as planned. Similarly, buyers often want to finance the purchase until they have had an opportunity to resell the item. Banks will charge large fees in addition to interest, on such short term trade finance loans. Once again, this is also similar to the financing PayPal now offers its online customers. Profits generated from providing trade finance are as enormous as the benefits to both the buyer and seller.

1433. Without a large international bank acting as a middleman in the sale of Iran's oil, Iran would have been forced to sell at a price below market to entice buyers to accept the increased risks associated with the parties dealing directly with each other.

1434. Without a large international bank providing trade finance for the sale of Iran's oil, many of Iran's customers would have found other sources of oil to purchase, as obtaining trade finance is essential to provide adequate working capital to most businesses.

1435. Some estimates report that up to 90 percent of world trade relies on one or more trade finance instruments.

1436. Most companies rely on external capital to finance large purchases of inventories, especially in situations where the exporting activity may also generate additional variable costs due to shipping, duties, storage, and freight insurance, which are generally incurred before export revenue is realized. In addition, ocean transit shipping times can be as long as several weeks, during which the exporting firm typically would be waiting for payment. All of these factors increase the need for working capital.

1437. As one can imagine, selling oil against international sanctions is a risky business. For the above listed reasons, a buyer may not be willing to send money to Iran, on a mere hope of someday receiving a supertanker full of oil. A typical supertanker carries approximately 2 million barrels of oil. The average price of oil during the Relevant Period was roughly \$60 per barrel. Therefore both the buyer and seller are at risk for \$120 million dollars. That is a strong incentive for both parties to take steps to ensure that each receives what they bargained for.

1438. Fortunately for State Sponsors of Terrorism, like Iran, there were a handful of banks more than willing to provide trade financing for them. It did not matter to Defendants that many of the parties to the trade were listed on OFAC's list of SDNs, or the underlying product being traded was subject to sanctions, as long as Defendants made money.

1439. Providing trade finance is a lucrative business. Defendants were able to mitigate the risk of others directly dealing with a State Sponsor of Terrorism by acting as the middleman.

The banks ensured that payments were processed without a hitch, and provided a level of trust and integrity to the transaction between the two parties that may not otherwise trust each other.

1440. Although the parties to the trade may not trust, or even know each other, large international banks often will have tools and resources at their disposal to perform adequate due diligence. Unlike Iran, HSBC has offices throughout the world.

1441. HSBC for instance advertises that it has offices in Iran, Iraq, Kuwait, Jordan, Qatar, Bahrain, Saudi Arabia, UAE, Oman and Turkey to name a few. HSBC has consistently won “Best Trade Finance Bank in the Middle East;” “Best Trade Bank in the Middle East and North Africa;” and “Leading Trade Services Bank in Asia Pacific, the Middle East & North Africa.”

1442. The Justice Department admitted why it decided to go soft on HSBC’s criminal conduct. It was worried that anything more than a wrist slap for HSBC might undermine the world economy. “Had the U.S. authorities decided to press criminal charges,” said Assistant Attorney General Lanny Breuer at a press conference to announce the settlement, “HSBC would almost certainly have lost its banking license in the U.S., the future of the institution would have been under threat and the entire banking system would have been destabilized.”

1443. A number of laws prohibit trade finance and USD clearing on behalf of Iran. For example, on April 7, 1980, the President, invoking the authority, *inter alia*, of the IEEPA and Section 301 of the National Emergencies Act (50 U.S.C. § 1631), issued Executive Order 12205 Prohibiting Certain Transactions With Iran including: The following acts, when committed by any person subject to the jurisdiction of the United States in connection with any transaction involving Iran, an Iranian government entity, an enterprise controlled by Iran, or any person in Iran:

- I. Making available any new credits or loans; . . .
- V. Make any payment, transfer of credit or other transfer of funds or other property or interests therein, except for purposes of family remittances.

**B. DEFENDANTS' AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY**

**1. Defendants Had a Duty to Ensure Their Acts Did Not Fund Terrorist Organizations and Knew of that Duty**

1444. Defendants agreed to provide Iran, Iranian entities, and Iranian SDNs with expert advice and financial services, as well as hundreds of billions of USD, money used to finance terrorist activities, including those that injured or killed Plaintiffs. Defendants agreed to provide that material support in violation of U.S. law and sanctions implemented to prevent Iranian entities from financing terrorist activities, including the Terrorist Attacks. Defendants participated by illegally providing hundreds of billions of USD over a decade-plus long period, which ultimately supported the Terrorist Groups. That participation earned Defendants a significant amount of profits—so much so that the companies agreed to forfeit billions to the U.S. government when they were caught and prosecuted. Defendants engaged in these transactions fully aware that the reason for the U.S. laws and sanctions they violated was to stop Iran from sponsoring terrorism.

1445. All banks which have international operations or relationships with correspondent banks have a duty, based on international banking norms, to adopt “Know Your Customer,” AML and anti-terrorist financing standards which are defined and enforced by the FATF and its supportive governments.

1446. The FATF is an intergovernmental body originally established by the 1989 Paris G-7 Summit to develop and promote standards and policies to combat money-laundering. The FATF includes 37 countries, 2 Observer countries, 9 international organization Associate Members, and 22 Observer Organizations, including the major financial center countries of

Europe, North America, and Asia. The United States and the United Kingdom are member jurisdictions of the FATF. Thus, Defendants are bound by these standards.

1447. According to its website, the FATF:

“...has developed a series of Recommendations that are recognised as the international standard for combating of money laundering and the financing of terrorism and proliferation of weapons of mass destruction. They form the basis for a coordinated response to these threats to the integrity of the financial system and help ensure a level playing field. First issued in 1990, the FATF Recommendations were revised in 1996, 2001, 2003 and most recently in 2012 to ensure that they remain up to date and relevant, and they are intended to be of universal application.

The FATF monitors the progress of its members in implementing necessary measures, reviews money laundering and terrorist financing techniques and counter-measures, and promotes the adoption and implementation of appropriate measures globally. In collaboration with other international stakeholders, the FATF works to identify national-level vulnerabilities with the aim of protecting the international financial system from misuse.”

1448. These standards are set forth in written principles issued by the FATF and the Basel Group of Bank Supervisors. They include a due diligence obligation to monitor publicly accessible information and allegations in relation to “high risk” customers, including charities collecting funds from the public.

1449. The duties owed under the FATF devolve upon officials and directors of all such banks, including Defendants.

1450. Combatting terrorist financing has been a priority for the FATF since 2001.

1451. The duty to monitor and profile charity customers arises independently of any particular transaction.

1452. Beginning with the creation of the FATF in 1989, and especially since the collapse of the Bank of Credit and Commerce International and the enactment of the first European Union directive on the subject in 1991, a consensus has evolved in the banking

community concerning knowing your customer and anti-terrorist financing standards required by international banking institutions.

1453. These standards are encapsulated in written principles issued by the FATF and the Basel Group of Bank Supervisors.

1454. In April of 1990, and updated in 1996 and 2003, the FATF issued a set of Forty Recommendations that establish a minimum for international AML standards and that has been endorsed by more than 13 countries. In October 2001, the FATF dealt specifically with terrorist financing by establishing a set of Eight Special Recommendations on Terrorist Financing, complementary to the Forty Recommendations. In particular, SR IV recommends that banks that “suspect or have reasonable grounds to suspect that funds are linked or related to, or are to be used for terrorism, terrorist acts or by terrorist organizations,” are required to report their suspicions to the proper authorities. The FATF Forty and the Eight Special Recommendations have been recognized by the International Monetary Fund and the World Bank as the international standards for combating money laundering and the financing of terrorism.

1455. Among the FATF’s Forty Recommendations regarding AML laws is Recommendation 15, as follows:

Financial institutions should develop programmes against money laundering and terrorist financing. These programmes should include:

- a) The development of internal policies, procedures and controls, including appropriate compliance management arrangements, and adequate screening procedures to ensure high standards when hiring employees;
- b) An ongoing employee training programme; and
- c) An audit function to test the system.

1456. In April 2002, the FATF issued a report entitled “Guidance for Financial Institutions in Detecting Terrorist Financing.” This report was issued to all major financial

institutions, including Defendants, to provide guidance to “ensure that financial institutions do not unwittingly hide or move terrorist funds. Financial institutions will thus be better able to protect themselves from being used as a conduit for such activity...”

1457. In addition to its inherent obligation not to violate criminal statutes of the United States, the FATF report very clearly put Defendants on notice of the risks to financial institutions from terrorist financing:

Regardless of whether the funds in a transaction are related to terrorists for the purposes of national criminal legislation, business relationships with such individuals or other closely associated persons or entities could, under certain circumstances, expose a financial institution to significant reputational, operational, and legal risk. This risk is even more serious if the person or entity involved is later shown to have benefited from the lack of effective monitoring or willful blindness of a particular institution and thus was to carry out terrorist acts.

1458. Further, the FATF warns that mere financial accounting and auditing might be insufficient protection against the abuse. “Direct field audits of programmes may be, in some instances, the only method for detecting misdirection of funds. Examination of field operations is clearly a superior mechanism for discovering malfeasance of all kinds, including diversion of funds to terrorists.” FATF Task Force on Money Laundering, Combating the Abuse of Non-Profit Organisations.”<sup>160</sup>

1459. There are also standards developed by the Wolfsberg Group of banks that affect the correspondent banks of Wolfsberg Group member financial institutions. Defendants Barclays, Credit Suisse, Deutsche, HSBC, and Standard Chartered are all members of the Wolfsberg Group.

---

<sup>160</sup> FATF, p. 3 (October 11, 2002).

1460. Due diligence is necessary when opening and maintaining accounts. According to the Wolfsberg AML principles,<sup>161</sup> global AML standards and guidelines established by the world's largest banks, a "bank will endeavor to accept only those clients whose source of wealth and funds can be reasonably established to be legitimate...Mere fulfillment of internal review procedures does not relieve the private banker of this basic responsibility."

1461. The Wolfsberg AML principles require that, for all accounts, the bank must exercise the following due diligence principles to identify the principle beneficial owners of an account:

- a) Natural persons: when the account is in the name of an individual, the private banker must establish whether the client is acting on his/her own behalf. If doubt exists, the bank will establish the capacity in which and on whose behalf the account holder is acting.
- b) Legal entities: where the client is a company, such as a private investment company, the private banker will understand the structure of the company sufficiently to determine the provider of funds, principal owner(s) of the shares and those who have control over the funds, e.g. the directors and those with the power to give direction to the directors of the company. With regard to other shareholders the private banker will make a reasonable judgment as to the need for further due diligence.
- c) Unincorporated associations: the above principles apply to unincorporated associations.

1462. To meet the due diligence standards established by the Wolfsberg AML principles, banks should meet the client before opening the account and must collect and record

---

<sup>161</sup> The Wolfsberg Group is an association of large global banks that came together in 2000, at the Chateau Wolfsberg in north-eastern Switzerland, which agreed to a set of global anti money laundering guidelines for international private banks. The banks initially involved included, but was not limited to, Barclays Bank, Credit Suisse Group, Deutsche Bank AG, Royal Bank of Scotland (ABN AMRO Bank) and HSBC. The Group's purpose is to develop financial services industry standards for "Know Your Customer," Anti-Money Laundering, and Counter Terrorism Financing Policies. The Wolfsberg Anti-Money Laundering Principles for Private banking were published in October 2000 (and revised in May 2002). In January 2002, the Group published a Statement on the Financing of Terrorism and, in November 2002, released the Wolfsberg Anti-Money Laundering Principles for Correspondent Banking. The Wolfsberg Group's most recent Statement, on Monitoring Screening and Searching, was published in September 2003. The standards are widely known.

the following information about each account: purpose and reasons for opening the account; Anticipated account activity; source of wealth (description of the economic activity which has generated net worth); estimated net worth; source of funds (description of the origin and the means of transfer for monies that are accepted for the account opening); and references or other sources to corroborate reputation information where available.

1463. On April 19, 2007, the Wolfsberg Group issued a statement “endorsing measures to enhance the transparency of international wire transfers to promote the effectiveness of global AML and anti-terrorist financing programs. The measures include both the development of an enhanced payment message format, which would include more detailed information about those conducting wire transfers in certain instances, as well as calling for the global adoption of basic messaging principles aimed at promoting good practice with respect to the payment system.” This statement was directed to the increasingly apparent risks inherent in MT 202 “cover payments” – one of the methods Defendants used to conceal their illegal USD funds transfers on behalf of Iran through the Eurodollar market.

1464. Defendants RBS, Barclays, Credit Suisse, and HSBC were all members of the Wolfsberg Group, and were listed on the April 19, 2007 press statement.

1465. In 1988, the Basel Committee, an international standards organization that formulates broad supervisory standards and guidelines and recommends statements of best banking practices, stated the following principles, among others:

- a) Banks’ management should ensure that business is conducted in conformity with high ethical standards and that laws and regulations pertaining to financial transactions are adhered to;
- b) Banks should not set out to offer services or provide active assistance in transactions which they have good reason to suppose are associated with money-laundering activities;

- c) Banks should cooperate fully with national law enforcement authorities to the extent permitted by specific local regulations relating to customer confidentiality. Care should be taken to avoid providing support or assistance to customers seeking to deceive law enforcement agencies through the provision of altered, incomplete or misleading information; and
- d) Where banks become aware of facts which lead to the reasonable presumption that money held on deposit derives from criminal activity or that transactions entered into are themselves criminal in purpose, appropriate measures, consistent with the law, should be taken, for example, to deny assistance, sever relations with the customer and close or freeze accounts.<sup>162</sup>

1466. The statutory and regulatory duties incumbent upon financial institutions operating in the United States are set out in the Bank Secrecy Act<sup>163</sup> and the regulations pertaining thereto. Other applicable industry standards support and clarify the duties of financial institutions, including Defendants.

1467. The Patriot Act, which amends the Bank Secrecy Act, was adopted in response to the September 11, 2001 terrorist attacks. The Patriot Act is intended to strengthen U.S. measures to prevent, detect, and prosecute international money laundering and the financing of terrorism.

1468. As a result of the Patriot Act, banks were required to establish AML programs, report suspicious activity, verify the identity of customers, and apply enhanced due diligence to certain types of accounts involving foreign persons.

1469. Although Defendants each established world class AML programs, each intentionally circumvented their own AML programs, in favor of Iran, for profit.

---

<sup>162</sup> Basel Committee, *Prevention of Criminal Use of the Banking System for the Purpose of Money-Laundering, State of Principles* (Dec. 1988), reprinted in BSA Manual, Section 1501.0 (September 1977).

<sup>163</sup> Titles I and II of Public Law 91-508, Oct. 26, 1970, as amended, codified at 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1959, and 31 U.S.C. § 5311 et seq.; Money Laundering Control Act (1986), 18 U.S.C. § 1956; The Money Laundering Prosecution Improvements Act, 31 U.S.C. §§ 5312, 5321; The Annunzio-Wylie Anti-Money Laundering Act (1992)(Pub. L. 102-550, Title XV, Oct. 28, 1992, 106 Stat. 4044), 31 U.S.C. 5318(h); The Money Laundering and Financial Crimes Strategy Act (1998), 31 U.S.C. §§ 5341(b) and 5342(b).

1470. Similarly OFAC of the U.S. Department of Treasury administers and enforces economic and trade sanctions against targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers. As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called SDNs.

1471. The law required Defendants to ensure that no wire transfers were made to or from any SDNs.

1472. Once again, despite being aware of their responsibility, and despite having both automated and manual systems in place to ensure that wire transfers are not made to SDNs, each of Defendants intentionally circumvented their own systems and as a result caused billions of dollars in wire transfers to be made to SDNs.

1473. Finally, the U.S. Department of the Treasury developed the Terrorist Finance Tracking Program to identify, track, and pursue suspected foreign terrorists, like Hamas and Hezbollah, and their financial supporters. Based on information that identifies an individual or entity, the U.S. Government is able to conduct targeted searches using records provided by SWIFT in order to trace financial transactions related to suspected terrorist activity. SWIFT information greatly enhances our ability to map out terrorist networks, often filling in missing links in an investigative chain.<sup>164</sup>

---

<sup>164</sup> U.S. Dep’t of the Treasury, *Terrorist Finance Tracking Program Fact Sheet* (June 23, 2006), <https://www.treasury.gov/press-release/Pages/js4340.aspx>.

1474. Despite the Treasury's best efforts to develop the Terrorist Finance Tracking Program, complete and accurate SWIFT data, supplied by banks, was a critical component relied upon by the Terrorist Finance Tracking Program and was crucial to the programs' overall effectiveness.

1475. Once again, despite being acutely aware of FinCEN's Terrorist Finance Tracking Program, and the effect that illegally altering SWIFT data would have on the effectiveness of the program, each of Defendants intentionally and routinely altered SWIFT data pertaining to billions of dollars of wire transfers thereby defeating the purpose of the Program.

1476. Unfortunately, almost all the tools developed by the U.S. government that used SWIFT data collection and analysis to stop terrorist financing all had the same Achilles heel – each relied on Defendants' integrity and compliance. Both of which were starkly absent during the Relevant Period.

1477. Each of the Defendants respective criminal pleas, DPAs, and/or settlements map out the period during which each participated in the Conspiracy, which corresponds to the period during which Iran was supporting and facilitating attacks in Iraq on the U.S. men and women stationed in Iraq, who are now Plaintiff's in this case.

1478. The Bank Secrecy Act and its regulations the Department of Treasury has issued apply to all financial institutions and specifically apply to banks, including Defendants. A principle purpose of the Bank Secrecy Act is to require financial institutions to maintain appropriate records and file certain reports which are particularly useful in investigating and uncovering money laundering, drug activities, terrorism and other illegal activities.

1479. The Bank Secrecy Act requires financial institutions operating in the United States, and their directors, to undertake a number of AML efforts to ensure that financial

institutions do not become conduits for terrorist financing or criminal proceeds, or facilitators of money laundering. Key provisions require financial institutions and their directors to establish AML programs that include explicit written policies and procedures which are approved by the banks directors with a notation of such approval in the minutes of the directors' meetings, to designate a qualified bank employee as the compliance officer with day-to-day responsibility for all aspects of the compliance program, to train employees, to establish an internal audit function, to verify the identity of persons seeking to open and maintain accounts (often termed "Know Your Customer" requirements), and to file reports identifying suspicious activities and currency transactions greater than US \$10,000 to guard against money laundering.

1480. In addition to the Bank Secrecy Act requiring financial institutions to implement AML procedures, international standards applicable to the financial services industry would similarly require implementations and enforcement of AML procedures. To the extent the United States has accepted membership or agreed to implement standards or principles of any organization promulgating such standards or principles, the standard or principles are requirements for financial institutions to conduct business in the United States.

1481. Financial institutions must ensure that appropriate bank personnel are trained in all aspects of the regulatory requirements of the Bank Secrecy Act and the banks internal compliance and AML policies and procedures.

1482. Non-profit organizations, particularly those held out as charitable organizations, constitute high-risk accounts warranting enhanced due diligence and scrutiny, because the mechanism of charitable fundraising has, "in numerous instances...been used to provide a cover for the financing of terror."

1483. According to the March 26, 2007 edition of *The Washington Post*, Defendants SCB, Commerzbank and the HSBC Defendants were among those briefed by U.S. government officials about the dangers posed (in terms of both proliferation and terror financing) in conducting business with Iran.

1484. The HSBC Defendants adopted all of the Wolfsberg standards by at least 2006.

1485. The SCB Defendants joined the Wolfsberg Group in 2015.

1486. Defendants were aware of each other's role in the Conspiracy because, among other facts, Defendants employed the same type methods to evade detection of their criminal activities, including wire stripping and non-transparent cover payments. Using those methods, Defendants provided Iran with access to billions of USD, without which it could not fund its terrorist acts, including those against Plaintiffs. Moreover, Defendants were aware of other banks providing banking services to sanctioned entities like Iran (e.g., Lloyds) because Defendants filled the void when those other banks ceased providing banking services to Iran.

## **2. Deutsche Bank AG's Participation in the Conspiracy**

1487. DB agreed to, and participated in, the Conspiracy.

1488. In furtherance of DB's illegal conduct described in this Complaint, which conduct was a cause of the Plaintiffs' injuries, damages, and losses, DB used its United States' branches/offices and various correspondent banks in New York to execute USD-denominated transactions requested by its customers, and specifically its customers in Iran.

1489. During the Relevant Period, and as part of its business in the United States, DB utilized its United States' offices/branches and correspondent banks to transfer money to certain charitable organizations that were actually Iranian Agents and/or Proxies, money which DB knew was being used to fund the Terrorist Attacks.

1490. In 2015, DB was fined \$258 million for violating OFAC regulations and U.S. sanctions by providing billions of dollars to Iran and other sanctioned entities.

1491. From at least 1999 through 2006, DB used non-transparent methods and practices to conduct more than 27,200 USD clearing transactions valued at over \$10.86 billion on behalf of entities subject to U.S. economic sanctions, including Iranian sanctioned entities.

1492. “Starting at least in 1999, [DB] employees recognized that U.S. sanctions rules, which applied at that time or over the course of subsequent years to Iranian, Syrian, Libyan, Burmese, or Sudanese customers or to customers who were listed on OFAC’s SDN list, would pose problems for USD payments sent to or cleared through the U.S., including clearing done through Deutsche Bank New York. Payments involving sanctioned entities were subject to additional scrutiny and might be delayed, rejected, or frozen in the United States. In order to facilitate what it saw as “lucrative” USD business for sanctioned customers, Bank employees developed and employed several processes to handle dollar payments in nontransparent ways that circumvented the controls designed to detect potentially-problematic payments.”<sup>165</sup>

1493. DB intentionally processed these illegal transactions in such a manner as to avoid detection by United States regulators and law enforcement. In particular, DB removed identifying information about Iran and Iranian entities from the SWIFT payment messages, used non-transparent cover payment methods that were stripped of important identifying information about the underlying party, and instructed Iranian clients to include notes or code words in requested payment transactions that would trigger “special processing” by DB employees to

---

<sup>165</sup> New York State Department of Financial Services, *In re Deutsche Bank AG, Deutsche Bank AG New York Branch Consent Order Under New York Banking Law §§ 39 and 44*, <http://www.dfs.ny.gov/about/ea/ea151103.pdf> (last visited Oct. 15, 2017).

ensure DB employees would hide identifying information to avoid having the payment requests picked up by DB New York personnel and OFAC filter software.

1494. As a result of this conduct, DB failed to maintain adequate and correct financial records of USD payment transactions and the omitted and modified payment requests set forth above likewise prevented DB New York from maintaining adequate and complete financial records as required by New York and United States law.

1495. One method that DB employed was wire stripping, or alteration of the information included on the payment message. Bank staff in overseas offices handling Message Type 103 serial payment messages, or MT 103s, removed information indicating a connection to a sanctioned entity before the payment was passed along to the correspondent bank in the U.S. With any potentially problematic information removed (or, as was done in some cases, replaced with innocuous information, such as showing the bank itself as the originator), the payment message did not raise red flags in any filtering systems or trigger any additional scrutiny or blocking that otherwise would have occurred if the true details were included.

1496. A second method was the use of non-transparent cover payments. The cover payment method involved splitting an incoming MT 103 message into two message streams: an MT 103, which included all details, sent directly to the beneficiary's bank, and a second message, an MT202, which did not include details about the underlying parties to the transaction, sent to DB New York or another correspondent clearing bank in the U.S. In this way, no details that would have suggested a sanctions connection and triggered additional delay, blocking, or freezing of the transactions were included in the payment message sent to the U.S. bank.

1497. DB employees recognized these handling processes were necessary in order to evade the sanctions-related protections and controls of DB New York and other correspondents.

For example, a relationship manager who handled significant business for Iranian customers explained the need for special measures as follows, in a 2003 email to colleagues: DB employs “specific precautionary measures that require a great deal of expertise” because “[i]f we make a mistake, the amounts to be paid could be frozen in the USA and/or DB’s business interests in the USA could be damaged.” Or, as the Assistant Vice President who oversaw payments processing explained to a colleague who inquired about Iranian payments, DB needed to employ “the tricks and cunning of MT103 and MT202” because of the U.S. sanctions restrictions otherwise applicable to sanctions-related payments.

1498. Therefore, as explained in another email summing up the process for handling Iran-related payments, DB’s preferred method was to process a payment using the cover payment method, and when that was not possible, “we will arrange for the order to be dropped . . . into a further repair queue, where the references to the principal will then be eliminated.”

1499. As new sanctioned customers were brought into the fold, or as newly-enacted U.S. sanctions programs affected existing customers, these processes were extended so as to ensure that payments did not encounter U.S.-based sanctions problems. For example, when DB staff learned that possible new U.S. sanctions might affect certain Syrian customers, they discussed how Syrian payment orders “must be ‘anonymised’ in the same way as orders from Iran or Libya, i.e. coverage without mention of Syria can be directed via USA and the order is made directly to the beneficiary’s bank.”

1500. On some occasions, payments that were rejected by DB New York due to a suspected sanctions connection were simply resubmitted to a different U.S. correspondent by the overseas office. Alternatively, some payments that were rejected in the U.S. when they were sent as MT 103 serial payments (which included details about the underlying parties) were then

resubmitted as MT 202 cover payments – in other words, because the information included on the more detailed message caused the rejection, the overseas office simply sent the payment again using the less transparent method.

1501. The special processing DB used to handle sanctioned payments was anything but business as usual; it required manual intervention to identify and process the payments that needed “repair” so as to avoid triggering any sanctions-related suspicions in the U.S. Indeed, on occasion, customers whose payments received this special processing questioned the extra fees the bank was charging for the manual processing. They were told that this is what was necessary in order to circumvent the U.S.-based sanctions controls.

1502. DB instituted a series of policies starting in 2006 to end these practices and wind down business with U.S.-sanctioned entities. However, some instances of resubmitting rejected payments or processing sanctions-related payments through New York persisted even after the formal policies were instituted.

1503. DB relationship managers and other employees worked with DB’s sanctioned customers in the process of concealing the details about their payments from U.S. correspondents.

1504. During site visits, in emails, and during phone calls, clients were instructed to include special notes or code words in their payment messages that would trigger special handling by the bank before the payment was sent to the United States. Sanctioned customers were told “it is essential for you to continue to include [the note] ‘Do not mention our bank’s name...’ in MT103 payments that may involve the USA. [That note] ensures that the payments are reviewed prior to sending. Otherwise it is possible that the [payment] instruction would be sent immediately to the USA with your full details. . . . [This process] is a direct result of the US

sanctions.” Customers, in turn, included notes in free-text fields of SWIFT messages such as “Please do not mention our bank’s name or SWIFT code in any msg sent via USA,” “PLS DON’T MENTION THE NAME OF BANK SADERAT IRAN OR IRAN IN USA,” or “THE NAME BANK MELLI OR MARKAZI SHOULD NOT BE MENTIONED . . . IMPORTANT: NO IRANIAN NAMES TO BE MENTIONED WHEN MAKING PAYMENT TO NEW YORK.”

1505. But DB did not rely on the customer notes and code words alone; DB’s payments processing staff were instructed to be on the lookout for any payment involving a sanctioned entity and ensure that no name or other information that might arouse sanctions-related suspicions was sent to the U.S. correspondents, even if the customer failed to include a special note to that effect.

1506. In fact, DB’s “OFAC-safe” handling processes and its experience in handling sanctions-related payments were selling points when soliciting new business from customers subject to U.S. sanctions. On one occasion, a relationship manager visiting a Syrian bank during a time when the U.S. was considering instituting certain Syrian sanctions pitched DB’s “OFAC-safe vehicles,” and when the client mentioned possibly splitting its business among several Asia-based banks, the relationship manager “highlighted that the Asian banks in general are not very familiar with OFAC procedures [and] [a]sked them to consider who their friends will be in the longer run, DB or Asian banks.” In another instance, after DB staff responded to a client inquiry about handling USD payments relating to Iran and Syria with a favorable “OFAC safe” solution, the Bank relationship manager reported the client was so pleased that it “used the opportunity to enquire whether we can also do USD payments into Burma/Myanmar.”

1507. The practice of non-transparent payment processing was not isolated or limited to a specific relationship manager or small group of staff. Rather, DB employees in many overseas offices, in different business divisions, and with various levels of seniority were actively involved or knew about it.

1508. In addition, some evidence indicates that at least one member of DB's Management Board was kept apprised about and approved of DB's business dealings with customers who were subject to U.S. sanctions.

1509. Certain non-U.S. employees, especially those who managed relationships with a high number of Iranian, Libyan, or Syrian clients or who regularly processed USD payments for sanctioned customers, were considered experts in the bank's "OFAC-safe" handling procedures. They regularly educated colleagues in other branches or in other divisions outside the U.S. about handling USD payments.

1510. Moreover, DB disseminated formal and informal written instructions emphasizing the need for utmost care to ensure that no sanctions-related information was included in U.S.-bound payment messages and setting out the various methods to use when processing sanctions-related payments.

1511. For example, DB staff told investigators that during the earlier part of the Relevant Period, an internal customer database included notes for certain sanctioned customers indicating their name must not be referenced in payment messages sent to the U.S.

1512. Later, DB payments processing employees prepared a training manual for newly-hired payments staff in an overseas office. The manual included a section titled "US Embargo Payments" that explained how to handle payments with a sanctions connection. An early draft included a warning, in bolded text: "Special attention has to be given to orders in which

countries/institutes with embargos are involved. Banks under embargo of the US (e.g., Iranian banks) must not be displayed in any order to [Deutsche Bank New York] or any other bank with American origin as the danger exists that the amount will be frozen in the USA.”

1513. A revised version of the payments manual admonished that payments from Iran and Syria “have to be treated with caution as [ ] the payment gets released from the queue; there is a probability the funds will be frozen by the Federal Reserve thereby causing financial and reputation loss for the Bank.” A later version of the manual noted the payment message might include key words such as “Embargo” or “Do not pay via US,” but it also cautioned employees that code words might not necessarily be present. In any event, non-U.S. employees were instructed that information linking a customer to a U.S. sanctions program must not be displayed in any message sent to DB New York or any other American bank. The preference, they were told, was to send two messages (that is, to use the cover payment method), but if that was not possible, they must reformat the message so that it gets routed for additional repair and reformatting “in such a way that the Embargo names are not visible to the receiving US banks.” The manual included computer screenshots illustrating how these problematic messages might appear and how to handle them.

1514. Moreover, less formal instructions were disseminated to certain staff via email throughout the Relevant Period. In one email chain regarding possible recruitment of a new customer with Libyan connections, DB staff were cautioned to “please be careful in regard to the US, since it does violate OFAC,” and were told, “please do not mention OFAC names in the subject line of e-mails!” In another instance, when certain U.S. regulations against a Syrian bank were imposed in 2004, relevant employees were told: “Let us be very careful while effecting

USD-denominated transaction[s] with Syria. In case we have to effect any USD-denominated remittance to Syria, please ensure that name of Syria should not appear in the message.”

1515. At the same time, DB staff took care to avoid publicizing details about their non-transparent payments handling, both within and outside the bank. Employees recognized the legal and reputational concerns and acted to keep the payment handling methods—and indeed the fact of the bank’s business dealings with sanctioned entities in general—on a need-to-know basis.

1516. For example, one non-U.S. relationship manager who asked for advice about USD processing was told, “Please be informed that any info on OFAC-safe business patterns (THAT DB does it and HOW DB does it) is strictly confidential information. Compliance does not want us to distribute such info to third parties, and forbids us explicitly to do so in any written or electronic form.” In another email, a senior compliance executive with oversight of this area told a non-U.S. relationship manager who was asking about the possibility of doing business with a Syrian customer that Compliance “agreed to do business on a low key level without public announcements etc.” Later, when that relationship manager was offering advice to another non-U.S. colleague about assisting a client who needed to make and receive USD payments with Iranian and Syrian connections, he cautioned his colleague: “As usual, let’s not revert to the client in writing due to the reputational risk involved if the e-mail goes to wrong places. Someone should call [the client] and tell them orally and ensure that the conversation is not taped. . . . Let’s also keep this e-mail strictly on a ‘need-know’ basis, no need to spread the news in [Deutsche Bank’s Asian offices about] what we do under OFAC scenarios.”

1517. Around the same time, that same relationship manager told another non-U.S. colleague: “Please note that while DB is prepared to do business with Syria, we obviously have

sizeable business interests in the US, too, which DB wants to protect. So any Syrian transaction should be treated STRICTLY confidential and should involve any colleagues on a ‘Must-Know’ basis only! . . . [W]e do not want to create any publicity or other ‘noise’ in the markets or media.”

1518. In addition, while one of the main purposes of the nontransparent practices was to keep the DB’s U.S. staff in the dark about the sanctions connections of the payments they were processing, DB New York staff occasionally raised objections to the Bank’s business relationship with U.S.-sanctioned parties based on U.S. law. Their European colleagues, however, did nothing to stop the practice but instead redoubled their efforts to hide the details from their American colleagues. For example, a relationship manager who did significant business with Iranian customers complained to his boss that colleagues in the Middle East “participated in a major conference call with senior management of [DB New York] and provided an overview of DB’s account activities with Syria outside the U.S. Senior management of [DB New York] complained strongly to DB Frankfurt that they see this as a breach of law.” The relationship manager viewed this incident not as a prompt to reexamine the bank’s business, however, but rather as indicating a need to better train the non-U.S. staff who handle the “very lucrative” Syrian and Iranian business to ensure such disclosures do not occur in the future.

1519. Based on the conduct described above, DB entered into Consent Orders with both the DFS and with the Board of Governors of the United States Federal Reserve System based on DB’s violation of New York and United States’ law. In conjunction with reaching these consent

orders, DB and DB New York agreed the facts alleged in the above paragraphs are true and correct.<sup>166</sup>

1520. Based on this and other illegal conduct on behalf of Iran aimed at the United States financial system, DB chose to enter into a sweeping consent order with the DFS for failing to maintain accurate books, accounts, and records in violation of New York Banking Law §§ 104, 200-c and 3 N.Y.C.R.R. 3.1 and failing to notify the State of New York or United States regulators upon the discovery of fraudulent conduct in violation of 3 N.Y.C.R.R. 300.1.

1521. In the Consent Order, DB agreed to:

- a) Pay a \$200,000,000 civil penalty to the State of New York;
- b) Implement an independent monitor, at its own expense but chosen by the State of New York, and who will report directly to the State of New York, whose job it will be to fully assess the (1) elements of DB's corporate governance system that contributed in any way to the improper conduct, (2) the thoroughness of DB's existing OFAC compliance mechanisms, (3) the organizational structure of the portion of DB's operations that deal with OFAC compliance, and (4) adequacy of any remedial efforts undertaken by DB;
- c) Fully cooperate with all state and federal regulators and the chosen independent monitor in their investigations into DB's money laundering on behalf of sanctioned entities, including Iran and Iranian entities;
- d) Develop an action Plan to address shortcomings identified by the independent monitor and submit this action plan to the State of New York;
- e) Allow the independent monitor to oversee the implementation of any corrective measures noted by the action Plan;
- f) Allow the independent monitor to assess compliance with the corrective measures noted in the action Plan and agree that all findings of the independent monitor in this regard will be submitted to the State of New York;

---

<sup>166</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Orders entered into between DB and the New York Department of Financial Services on or about November 3, 2015, as if fully set forth herein.

- g) Fire, and not rehire, a number of employees who were directly involved in the illegal USD transactions on behalf of Iran and Iranian entities; and
- h) That DB remains subject to prosecution by the State of New York should DB materially breach the terms of this Consent Order.

1522. Based upon the conduct described herein, the United States Federal Reserve also investigated DB's conduct with respect to violations of the Trading with the Enemy Act (50 U.S.C. §§ 5, 16) and the IEEPA (50 U.S.C. §§ 1701-06) and found sufficient grounds to compel DB to enter into the Cease and Desist Order.<sup>167</sup>

1523. Based on the conduct described herein, DB also agreed to the following terms with the United States Federal Reserve:

- a) Pay a \$58 million penalty to the Federal Reserve; and
  - i. Implement a timetable for full compliance with OFAC regulations;
- b) Submit a proposed program, subject to approval by the Reserve, designed to:
  - i. Provide an annual assessment to the Reserve of OFAC compliance risks posed by DB's customer base;
  - ii. Global policies and procedures for DB and all its subsidiaries regarding OFAC compliance;
  - iii. The establishment of a uniform OFAC compliance system that is widely publicized throughout the organization;
  - iv. Ensure that DB's OFAC compliance measures are adequately staffed and funded;
  - v. Training for DB employees that have responsibilities for OFAC compliance that is tailored to their particular job level;
  - vi. Establish an audit program designed to test for OFAC compliance; and

---

<sup>167</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Orders entered into between DB and the United States Federal Reserve System on or about November 4, 2015, as if fully set forth herein.

vii. Establish an annual OFAC compliance review that will be conducted by a third party as approved by the Reserve and that will be submitted to the Reserve within 90 days of completion.

1524. The services provided by DB to Iran and its Agents and Proxies consist of the provision of USD funds, expert advice, and/or financial services described above.

### **3. The HSBC Defendants' Participation in the Conspiracy**

1525. The HSBC Defendants agreed to, and participated in, the Conspiracy.

1526. Beginning by at least the mid-1990s and continuing through at least 2006, the HSBC Defendants had a continuous, ongoing relationship with Iran and its Agents and Proxies.

1527. In furtherance of the HSBC Defendants' illegal conduct described in this Complaint, which conduct was a cause of the Plaintiffs' injuries, damages, and losses, the HSBC Defendants used their United States branches/offices and various correspondent banks, in New York to execute USD-denominated transactions requested by its customers, and specifically its customers in Iran.

1528. During the relevant times described in this Complaint and as part of its business in the United States, the HSBC Defendants utilized their United States' offices/branches and correspondent banks to transfer money to certain charitable organizations that were actually Iranian Agents and/or Proxies, which money the HSBC Defendants knew was being used to fund the Terrorist Attacks that are the subject of this Complaint.

1529. From at least 2000 through 2006, the HSBC Defendants used non-transparent methods to conduct illegal transfers valued at over \$660 million, including approximately \$183 million of transactions with Iran, a significant portion of which was used by Iranian-sponsored Terrorist Groups for purposes of committing the subject Terrorist Attacks.

1530. Each such transfer was initiated by the HSBC Defendants and routed through a correspondent bank account in the United States for the benefit of the Iran and its Agents and

Proxies and resulted in those Terrorist Groups being provided with material support that allowed them to perpetrate the acts of international terrorism identified herein.

1531. These transfers not only overlapped with the Terrorist Attacks perpetrated by Terrorist Groups that killed, maimed, or otherwise injured Plaintiffs and Plaintiffs' family members, but also occurred at a time when the HSBC Defendants knew that funds they transferred on behalf of Iran or Iran's Agents and Proxies, as each such transfer of funds was for the benefit of the Terrorist Groups and resulted in those Terrorist Groups being provided with material support that allowed them to perpetrate the acts of international terrorism identified herein.

1532. Further, the HSBC Defendants knew that such transfers were funding the terrorists responsible for the Terrorist Attacks.

1533. In 1999, HSBC Group established a relationship with the Tehran office of Bank Melli Iran, and it launched an "Iran Representative" office in Tehran, Iran that same year.

1534. In December 2000, HSBC Group members entered into a \$500 million project finance agreement with six Iranian commercial banks: Bank Saderat Iran, Bank Melli Iran, Bank Mellat, Bank Tejarat, Bank Sepah and the Export Development Bank of Iran.

1535. Beginning in the late 1990s, Defendants HSBC-Europe and Defendants HBME devised a procedure whereby Defendants and/or unnamed co-conspirators put a cautionary note in their SWIFT-NET payment order messages including language such as, "care sanctioned country," "do not mention our name in NY," and "do not mention Iran."

1536. Eurodollar payment transactions with these cautionary notes automatically fell into what Defendants HSBC-Europe termed a "repair queue," where employees of HSBC-

Europe and HBME manually removed all references to Iranian-sanctioned entities from the SWIFT-NET messages associated with each transaction.

1537. Removing those references helped ensure the transactions would not be flagged as potentially suspect and would be processed by U.S. banks and financial institutions.

1538. Between 2001 and 2007, the HSBC Defendants actively participated in the Conspiracy by repeatedly undertaking various methods to facilitate Eurodollar payments, trade finance and foreign exchange transactions on behalf of Iran and its Agents and Proxies through the United States that would evade U.S. sanctions by disguising Iran's financial activities as its USD funds were cleared and settled by U.S. financial institutions, including Defendants HSBC-US.

1539. Unlawful Iranian transfers of USD funds from HSBC-Europe and HBME were sent through the HSBC Group's USD correspondent accounts at HSBC-US by: (1) deleting references to Iran from the payment instructions (a.k.a. "stripping" the transactions), or otherwise altering the SWIFT-NET messages, to either omit or falsify information that would have otherwise indicated Iran's involvement in the transaction; and (2) styling transactions as bank-to-bank "cover" transactions between two non-Iranian banks, solely because the MT 202 payment order message format used for such transactions did not expressly obligate HSBC to identify the transaction's originator and beneficiary, thus avoiding any disclosure of the transaction's Iranian connections, and blocking HSBC-US's electronic filter algorithms from recognizing the transaction, let alone assessing whether it qualified for any OFAC exemption or license.

1540. Defendants HSBC-Europe created detailed plans to avoid triggering HSBC-US's automated OFAC filter software and reduce the need for "manual intervention" (e.g. the reformatting Eurodollar transactions), thus sparing HSBC-Europe's employees from the need to

manually alter the SWIFT-NET messages in order to remove references that might otherwise identify the presence of Iranian parties to the transaction, and associated scrutiny.

1541. This enabled the HSBC Defendants' business with Iran in the Eurodollar market to proceed quickly and profitably.

1542. In 2010, facing U.S. government investigations, HSBC-US hired Deloitte LLP as its outside auditor to identify and examine HSBC Group's OFAC sensitive USD funds transactions involving Iran and other prohibited countries or persons that went through the bank.

1543. That "review" identified more than 25,000 illegal transactions that involved Iran, worth a total of more than \$19.4 billion in USD funds.

1544. The payment orders had been sent to HSBC-US and other financial institutions in the United States without referencing Iran, ensuring the Eurodollar payment transactions would be processed without delay and not be blocked nor rejected by the algorithms in the automated OFAC filtering systems.

1545. The HSBC Defendants deliberately amended SWIFT-NET payment order messages and used MT 202 cover payments to conceal the nature of the transactions from HSBC-US automated OFAC sanction screening filters and those of other financial institutions in the United States, and HSBC-US was aware the other HSBC Defendants used such methods to alter payment order messages.

1546. At the same time, the HSBC Defendants provided expert advice, training, mentoring, and educated their Iranian co-conspirators on how to deceptively format SWIFT-NET payment order messages, *inter alia*, to avoid detection and scrutiny by OFAC and other U.S. financial institutions.

1547. The HSBC Defendants' (and other Defendants' and co-conspirators') willingness to process payments in this manner enabled Iran to flood the global financial system with undetectable USD payment transactions and effectuate—what would have otherwise been preventable—transfers of USD funds to the Terrorist Groups, including those responsible for perpetrating the Terrorist Attacks.

1548. Defendants HSBC Holdings was aware of Defendants HSBC-Europe and HBME's involvement in the Conspiracy with Iran as early as 2000.

1549. For example, HSBC Group AML Compliance Head Susan Wright received an email on June 9, 2000, from Bob Cooper, an HSBC colleague, informing Wright of an existing procedure the HSBC Defendants were already employing to avoid OFAC filter detection.

1550. Cooper explained: (1) a client bank had been “automatically replacing a remitter’s name with that of” the client bank and that bank was utilizing bank-to-bank “cover payments” because the payment message formats did not expressly require identification of either the underlying party originating the transaction or the transaction’s ultimate beneficiary; (2) in the future, for OFAC sensitive transactions, that bank would “arrange cover for the payment using MT202/203 remittances;” and (3) that bank planned to send a separate ‘MT100 message’ to the recipient bank, providing full payment details for the originator and ultimate beneficiary.

1551. Cooper’s email acknowledged that “[i]n this way a payment in US\$ can be made for an individual or company on the OFAC list, without the name being ‘detected’ by the OFAC filters that all US banks would apply.”

1552. Several days later, on June 14, 2000, Wright forwarded Cooper’s June 9, 2000 email to the then-current Head of HSBC Group Compliance, Matthew King.

1553. In her cover email, Wright stated the “practice” detailed by Cooper was “unacceptable” and informed King that it was her position that: (1) “We advised them that this was contrary to SWIFT guidelines (drawn up to address FATF concerns re money laundering via wire transfers) which required that the full details (names and addresses) of remitters and beneficiaries are included;” and (2) “From a Group perspective I consider the continuation of this practice [the client bank’s future plan to conceal OFAC sensitive transactions behind bank-to-bank transfers] to be unacceptable as a deliberate and calculated method to avoid US OFAC sanctions and has the potential to raise serious regulatory concerns and embarrass the Group.”

1554. Senior HSBC Group officials were aware of the Conspiracy, including the specific methods and overt acts by which Iran, the Iranian banks and the HSBC Defendants were carrying it out.

1555. However, despite this awareness, senior compliance officials of HSBC Group and its subsidiary banks and entities (including compliance officials at Defendants HSBC Holdings, HSBC-Europe, HBME, and HSBC-US) did not put an end to this illicit banking “practice” with Iran. Instead, with clear knowledge of its purpose—and awareness that other banks participated in the Conspiracy—they knowingly employed similar techniques to evade OFAC requirements, thus allowing the HSBC Defendants to continue deploying and refining their respective “procedures” to facilitate illegal Eurodollar payments from and for Iran in USD funds.

1556. In late 2000, in coordination with the CBI, HSBC signed a project finance framework agreement with six Iranian commercial banks: including Bank Melli, Bank Saderat, Bank Mellat, Bank Tejarat, Bank Sepah, and the Export Development Bank of Iran.

1557. In or around January 2001, Bank Melli’s London branch maintained Eurodollar accounts with several other major international banks, but was interested in establishing a

relationship with HSBC that would give HSBC the majority of Bank Melli's USD funds clearing and settlement business.

1558. In an April 30, 2001 letter, Defendants HSBC-Europe presented Bank Melli in London with a proposal (the "Bank Melli Proposal") for processing Bank Melli payments. HSBC-Europe's proposal boasted that HSBC-Europe was "confident that we have found a solution to processing your payments with minimal manual intervention."

1559. The Bank Melli Iran Proposal expressly underscored that, if it adopted HSBC-Europe's "solution," Bank Melli would not be identified as a sender in any payment order message and, thus, HSBC-Europe would ensure that Iranian transactions involving USD funds would not run into any 'speed bumps' or other obstacles.

1560. The "solution" provided specific alternative wording, as it explained: "The key is to **always** populate field 52 – if you do not have an ordering party then quote 'One of our Clients,' **never leave blank**. This means that the outgoing payment instruction from HSBC will not quote 'Bank Melli' as sender – just HSBC London and whatever is in field 52. This then negates the need to quote 'DO NOT MENTION OUR NAME IN NEW YORK' in field 72." (Emphasis in original).

1561. HSBC-Europe's proposal further requested, "In order to test our proposed solution we would appreciate if you used the following templates when submitting your next payments to the following customer, or alternatively submit a USD 1 test payment" and provided the following:

MT202

20: Your Ref....

21: Related Ref....

32: Amount/currency/Value date....

50: **DO NOT QUOTE IF IRANIAN**

52: Customer Name OR One of our clients MUST BE COMPLETED

53: /68296908  
54:  
56:  
57: Beneficiary Banker (SWIFT codes where possible)  
58: Beneficiary (SWIFT codes where possible)  
70: Any Payments details for beneficiary...  
72: **Please leave blank**  
**MT100**  
Pay as above.

(Emphasis in the original.)

1562. Thus, the Bank Melli Proposal documented the HSBC Defendants' active coordination and participation in the Conspiracy to illegally remove, omit or falsify essential information from SWIFT-NET messages so as not to trigger OFAC sanctions screening filters or otherwise permit HSBC-US or other U.S. depository institutions to detect Iranian transactions in USD funds.

1563. An internal HSBC memorandum that was associated with the Bank Melli Proposal also makes clear HSBC's awareness of Defendant SCB's role as NIOC's primary (Western) banker at the time.

1564. In 2001, John Wilkinson served as HSBC-Europe's Institutional Banking Relationship Manager for HSBC-Europe's Bank Melli account.

1565. In a June 28, 2001 email titled "Re: Bank Melli" to HSBC-US, Wilkinson discussed the Bank Melli Proposal, describing HSBC-Europe's "usual method" to alter the wording of Iranian payment order messages, and the rationale for doing so. "Once the proposition goes live, we have instructed Bank Melli to alter the format of its payments to achieve straight through processing. The field 52 input of 'one of our clients' is a standard phrase used by MPD [Multicurrency Payments Department] in these situations." "Since sending the letter we have further asked them to only put 'One of our clients' in field 52, thus removing the

chance of them inputting an ‘Iranian referenced’ customer name, that causes fall out of the cover payment sent to HSBC-US and a breach of OFAC regulations.”

1566. In further support of his position to continue this standard ‘procedure,’ Wilkinson explained that a payment involving an Iranian bank had been blocked because HSBC-Europe’s MPD [Multicurrency Payments Department] “failed to spot the poor input and did not follow the normal procedure of altering the payment.”

1567. In other words, the HSBC Defendants’ “normal” procedure was to conspire with Iranian banks, including Bank Melli, to deliberately alter payment order messages prior to sending them to the United States for the express purpose of avoiding detection and analysis by U.S. banks, regulators and law enforcement.

1568. In an email exchange in October 2001 between David Bagley, Defendants HSBC Middle East’s Regional Head of Legal and Compliance, and Matthew King, a member (and later Head of) HSBC Group’s Audit Department, King noted:

We also have to bear in mind pending US legislation which will in effect give the US extraterritorial authority over foreign banks, particularly if we are unfortunate enough to process a payment which turns out to be connected to terrorism. My own view therefore is that some of the routes traditionally used to avoid the impact of US OFAC sanctions may no longer be acceptable.

1569. HSBC Group AML Head Susan Wright and Money Laundering Control Officer John Allison received copies of King’s e-mail.

1570. King’s email further confirms that senior executives and managers within the HSBC Group comprehended what the HSBC Defendants (and other foreign banks) had “traditionally” been doing for years when they used “routes” (a euphemism for altering payment order messages prior to routing them to U.S. financial institutions through SWIFT-NET) to avoid

disclosing a transaction's Iranian connections, and that some of those transactions might prove to be "connected to terrorism."

1571. A January, 2003 memorandum authored by HBME and disseminated to other members of the HSBC Defendants confirms not only the HSBC Defendants' ongoing participation in the Conspiracy, but also their knowledge of the participation of other co-conspirators, and Iran's desire to further evade U.S. sanctions.

1572. The memorandum stated in relevant part the following. "It is believed that some service providers amend the payments to ensure Iran is not mentioned in the body of the payment instruction to their USD correspondent. This process minimizes the risk of payment being referred to OFAC." "Currently, it is estimated that Iranian banks issue up to 700 USD payments a day using their USD providers, mainly banks in the UK and Europe, which in turn use their New York USD correspondents to effect [sic] the payments."

1573. In addition to acknowledging the existence of the Conspiracy, the HBME memorandum also advised:

"[T]here is substantial income opportunity to sell a USD payments proposition to Iranian banks in view of the impending FATF regulations...The [requirements of the] new regulations...increases the risk of Iranian payments being held in the USA as they may fall foul of the OFAC regulations. The Iranian Banks have now prioritized this issue and are now actively seeking a solution from their banks, including HSBC."

1574. From at least 2003 forward, HSBC provided banking and payment services in the Eurodollar market to, among other Iranian entities, the NIOC (which, as noted previously, was later designated pursuant to Executive Order 13382 and identified as an agent or affiliate of the IRGC during the Relevant Period). The HSBC Defendants also provided Eurodollar, trade-finance, and foreign exchange services for NIOC.

1575. Over the course of the next several years, the HSBC Defendants continued their participation in the Conspiracy.

1576. In an October 9, 2006 email, David Bagley [HBME's Regional Head of Legal and Compliance] informed senior HSBC Group officials that key U.S. policymakers were "...in favour of withdrawing the U-turn exemption from all Iranian banks. This on the basis that, whilst having direct evidence against Bank Saderat particularly in relation to the alleged funding of Hezbollah, they suspected all major Iranian State owned banks of involvement in terrorist funding and WMD [weapons of mass destruction] procurement."

1577. Further demonstrating his awareness of the risks HSBC was engaged in with Iran, Bagley was listed as the contact person on the April 19, 2007 Wolfsberg Group press release calling for more transparency for international wire transfers "to promote the effectiveness of global anti-money laundering and anti-terrorist financing programs."

1578. Eight months later, in a June 8, 2007 email, Bagley informed HSBC Holding's CEO, Michael Geoghegan, and others, that "[U.S. Treasury Under Secretary for Counter Terrorist Financing and Sanctions] Levey essentially threatened that if HSBC did not withdraw from relationships with [redacted] we may well make ourselves a target for action in the US."

1579. Bagley's email thus confirmed that various relationships continued to exist in the Eurodollar market with Iran and Iranian banks, including Bank Saderat.

1580. Bagley not only acknowledged that HSBC had "...an agency banking relationship in HSBC-EUROPE both for [redacted] and other Iranian banks," but he confessed that "[t]here are further complications surrounding the process of closure with all Iranian banks as we have some USD 9m in reimbursements due from Sepah, where we are running off trade lines, where we may need cooperation from Central Bank of Iran."

1581. On December 11, 2012, the U.S. DOJ announced that Defendants HSBC Holdings and HSBC-US had admitted to AML and OFAC sanctions violations, and had agreed to enter into a DPA and pay a \$1.256 billion forfeiture. As explained further infra, the DOJ issued a press release announcing the DPA, and summarizing the HSBC Defendants' illegal conduct.<sup>168</sup>

1582. In connection with the DPA, the DOJ filed a four-count felony criminal information against HSBC Holdings and HSBC-US, charging them with: (1) willfully failing to maintain an effective AML program; (2) willfully failing to conduct due diligence on their foreign correspondent affiliates; (3) violating the IEEPA; and (4) violating the Trading with the Enemy Act. HSBC Holdings and HSBC-US waived federal indictment, agreed to the filing of the information, and claimed to have accepted responsibility for HSBC's and its employees' criminal conduct.

1583. Despite its agreement to overhaul its U.S. and global compliance functions, HSBC remained a conduit for illicit funds.

1584. On December 9, 2010, the U.S. Treasury Department designated Tajco, describing it as "a multipurpose, multinational business venture involved in international trade as well as real estate and presided over by Ali Husayn and Kassim Tajideen.... Since at least December 2007, Ali Tajideen used Tajco Sarl, operating as Tajco Company LLC, as the primary entity to purchase and develop properties in Lebanon on behalf of Hizballah."

1585. The designation also covered Kairaba Supermarket, a subsidiary business of Tajco Ltd.

---

<sup>168</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPA entered into between the HSBC Defendants and the DOJ on or about December 11, 2012, as if fully set forth herein.

1586. A July 13, 2012 article published by Reuters entitled “Special Report: HSBC’s Money-Laundering Crackdown Riddled With Lapses” reported that an HSBC-US compliance officer had identified suspicious transactions involving Hezbollah, specifically Tajco and Kairaba Supermarket.

1587. In December 2013, the Treasury Department announced that Defendants HSBC-US agreed settle potential civil liability for three apparent violations of the Global Terrorism Sanctions Regulations, 31 C.F.R. Part 594.

1588. The fine reflected the fact HSBC-US facilitated transactions in late 2010 and early 2011 that benefited Tajco.

1589. This facilitation of terrorism financing for Hezbollah a considerable time after Defendants HSBC Holdings and HSBC-US began negotiating their deal with the DOJ, strongly suggests that, as of early 2011, the HSBC Defendants had not seriously remediated their AML and combating the financing of terrorism controls and procedures, even after being caught committing hundreds of felonies.

1590. As alleged in greater detail below, even though at all relevant times Defendants HSBC-US was aware that: the HSBC Defendants were participating in the Conspiracy to unlawfully transmit Iranian USD funds through U.S. banks (including HSBC-US); and periodically complained about Defendants HBME and HSBC-London’s conduct and proposed new procedures and policies for HSBC Group members that would have provided HSBC-US improved transparency, HSBC-US took no measures to prevent HSBC-US from facilitating hundreds of millions of dollars of payments to Iran in violation of 18 U.S.C. § 2332d. Accordingly, in addition to violating § 2332d, HSBC-US’s conduct evidenced its agreement to continue participating in the Conspiracy despite its complaints, its knowledge or deliberate

indifference to the Conspiracy's criminal objectives and purposes, and its commission of multiple overt acts in furtherance of the Conspiracy.

1591. One key example of HSBC-US's failure to take substantive measures to ensure that it would not facilitate the HSBC Defendants' provision of illegal material support and services to Iran is reflected in a July 12, 2001 e-mail to senior employees at HSBC-US (containing a memorandum authored by HSBC Group Representative for Iran, John Richards).

1592. Richards's memorandum outlined the business opportunities members of the HSBC Group were presented with in connection with prospects to expand and grow HSBC Group's relationships with Iran, the CBI and Bank Melli, explaining: "We have been approached by the Central Bank of Iran to take back their USD clearing business from Natwest. In principal I am keen to do this but on the clear proviso that it can be done profitably and on a sustainable basis." "One of our key objectives for the year is to develop HSBC's Asset Management activities in Iran and with the Central Bank now managing the oil price stabilization fund amounting to some USD10bn there is considerable scope for this. Obviously, many foreign banks are chasing the same business and so we need to demonstrate some competitive or relational advantage. The proposal from the Central Bank was therefore not unwelcome...The Central Bank manages their transactions through Bank Melli London..." "In summary if we can make this business independently profitable and sustainable the benefits that we can derive particularly from the Treasury Asset Management and Investment spin offs will be substantial."

1593. Richards's memorandum also demonstrates the HSBC Defendants' awareness that other foreign banks (including Defendants) were eagerly pursuing USD clearing and settlement business with the CBI in the Eurodollar market.

1594. On July 12, 2001, Denise Reilly, HSBC-US's Senior Manager in Payment Operations, sent an e-mail titled "Re: Bank Melli" to various senior HSBC-US employees in which she stated, "It was relayed to us that the Group (with the Backing of Bond) [the Chairman] was looking to significantly grow our presence in Iran." Reilly also explained the "current lines of credit [for Iran] were reported to be \$800m, trade lines of \$150m and growth was anticipated in trade, cash management and internet banking."

1595. Thus, HSBC-US senior employees understood the significance to the HSBC Defendants of their Iranian business and specifically, the HSBC Defendants' relationship with Bank Melli.

1596. As early as 2001, senior HSBC-US payments, compliance and business managers were informed that Iranian Eurodollar payment transactions were being sent by Defendants HSBC-London to HSBC-US for clearing and settlement in USD funds after references to Iran had been deleted.

1597. HSBC-US employees were also informed of an HSBC-London proposal to streamline the processing of Iranian U-turn transactions by omitting references to Iran so the payment orders would not be halted by OFAC's sanctions screening filter in the United States. Emails at the time show that senior HSBC-US officials expressed discomfort with the HSBC-London proposal, but took no other action to stop or prevent the activity already occurring.

1598. As noted above, a senior HSBC-US employee received an e-mail on June 28, 2001 titled "Re: Bank Melli," which described HSBC-London's "usual method" of altering payment order messages and the reasons for doing so.

1599. Another example of HSBC-US's knowledge and acquiescence in the Conspiracy is memorialized in a November 14, 2002 memorandum entitled "COMPLIANCE-OFAC

ISSUES IN GENERAL AND SPECIFIC TO IRAN” authored by HSBC-London’s Multicurrency Payments Department Head Malcolm Eastwood (“the Eastwood Memorandum”).

1600. The Eastwood Memorandum was sent to both HSBC-US and HSBC-London employees and forwarded to additional HSBC-US employees in separate emails.

1601. The Eastwood Memorandum discussed both HSBC’s “cover payment method” of evading U.S. sanctions and the specific actions taken by HSBC to modify the contents of payment messages. In relevant parts, the Eastwood Memorandum stated:

- a) “As the custodian of HSBC-Europe’s payments operation I currently feel that we may be exposing ourselves to unnecessary and unacceptable Reputational and Operational Risk when we are handling payments originating from FIs [financial institutions] domiciled in or who are a local branch of an FI domiciled in an OFAC regulated country.”
- b) “HSBC-Europe’s historical practice has been to send these types of payments where the U Turn principal applies (ie funds are generally moving from a European bank to another European bank for the credit of an OFAC regulated entity) via the Cover Payment method. This means the payment instructions received by HSBC-US contains no mention of the country or entity involved. My understanding is that this has been accepted practice for many years and that HSBC-Europe IBL hold accounts, some in USD for FIs domiciled in these countries i.e. Cuban, Iranian etc.
- c) “The Iranian banks continue to send us what I describe as conditional payment instructions which for HSBC-Europe require an element of amendment by ourselves. This introduces operational risk and under FATF principles we should not be amending these payments instructions. Acceptance of these items over many years means that we are bound by the precedents currently in place, and I believe that we need to break these precedents...”
- d) “[W]e need...[t]o agree a ‘template’ payment instruction for these U Turn Payments which can be used by [Payment and Cash Management] Sales and the RM team and sent to the Iranian Banks stipulating that payments must be formatted in this way, confirming that we will be sending these via the Serial method and that any deviation from this template will be at the Iranian Banks own risk.”
- e) “Whilst I am told that there are significant business opportunities particularly with countries such as Iran there are also substantial Reputational and Operational Risks, not to mention financial losses associated with it.”

1602. In addition, HSBC-US's OFAC filter occasionally stopped an Iranian-related transaction, sent by an HSBC Group affiliate, in which the identifying information had inadvertently been retained, demonstrating that undisclosed Iranian U-turn exemption transactions continued to be sent through HSBC-US correspondent accounts.

1603. HSBC-US employees were copied on similar memoranda issued by other HSBC Defendants during the Relevant Period. For example, a January 2003 memorandum circulated by HBME (and received by several HSBC-US employees) also noted that “[t]he Group now has an excellent relationship with all Iranian banks and some very larger Iranian corporates such as National Iranian Oil Co, National Petrochemical Co, National Iranian Gas Co, National Iranian Steel Co, top Iranian insurance companies, Ministry of Power, Ministry of Post and Telecommunications, etc.”

1604. The memorandum also confirmed the HSBC Defendants' awareness that other non-Iranian banks were participating in the Conspiracy, stating:

- a) “It is believed that some service providers amend the payments to ensure Iran is not mentioned in the body of the payment instruction to their USD correspondent. This process minimizes the risk of payment being referred to OFAC.”
- b) “Currently, it is estimated that Iranian banks issue up to 700 USD payments a day using their USD providers, mainly banks in the UK and Europe, which in turn use their New York USD correspondents to effect [sic] the payments.”
- c) “[T]here is substantial income opportunity to sell a USD payments proposition to Iranian banks in view of the impending FATF regulations...The [requirements of the] new regulations...increases the risk of Iranian payments being held in the USA as they may fall foul of the OFAC regulations. The Iranian Banks have now prioritized this issue and are now actively seeking a solution from their banks, including HSBC.”

1605. An October 2003 document entitled “IRAN-STRATEGY DISCUSSION PAPER” circulated to senior HSBC-US employees further documented the HSBC Defendants’

eagerness to facilitate USD funds transfers for Iran, noting: “One of the reasons to accelerate our process of engagement is to demonstrate, to the authorities within Iran, that we are committed to the development of their country. This is seen to be particularly important given the more aggressive/pragmatic approach to Iranian business adopted by French and German competitor banks.”

1606. Nevertheless, despite being copied on such memos, HSBC-US took no further action to stop the unlawful activities.

1607. Even when HSBC-US blocked Iranian payment transactions, it failed to take further action to ensure that other HSBC Defendants would not continue these illegal practices.

1608. For example, in late December 2002, HSBC-US’s OFAC sanctions screening filter stopped and rejected a payment order listing Bank Melli as the originator of the SWIFT-NET message that contained a field that read, “Do not mention our name in NY.”

1609. An internal HSBC-US email dated December 30, 2002, informed HSBC-US’s compliance team about the Bank Melli payment, which once again confirmed the HSBC Defendants’ ongoing process of altering payment order messages.

1610. On June 13, 2003, HSBC-US’s OFAC filter stopped another transaction, this time for \$150,000 in USD funds, because it included both a reference to Bank Melli and the words “do not mention our name.”

1611. In a June 16, 2003 email entitled “PLC-Re do not mention our name,” HSBC-US compliance officers were notified about the June 13 blocked transaction and received additional confirmation of the HSBC Defendants’ illegal practice of altering fields within Iranian payment order messages for the express purpose of escaping detection in the United States.

1612. During 2004, in furtherance of the Conspiracy, HSBC Group members sent approximately 7,000 Iranian Eurodollar transactions through various SWIFT-NET network accounts for clearance and settlement by Defendants HSBC-US and other correspondent banks in the United States without disclosing their source.

1613. HSBC-US did not report any of the HSBC Defendants' illegal conduct involving Iran to any of its regulators or to U.S. law enforcement at that time.

1614. During 2005, in furtherance of the Conspiracy, HSBC-London and HBME together sent about 5,700 Iranian Eurodollar transactions through various SWIFT-NET network accounts for clearance and settlement by Defendants HSBC-US and other correspondent banks in the United States without disclosing their source.

1615. On April 19, 2005, HSBC-US's OFAC filter again stopped a \$362,000 payment order from Bank Melli because it contained the phrase "do not mention our name in New York."

1616. HSBC-London re-submitted the same payment on April 22, 2005, but HSBC-US stopped it again, this time sending HSBC-London a SWIFT-NET message requesting full disclosure of the name and address of the underlying originator and ultimate beneficiary of the USD funds.

1617. In early May 2005, HSBC-US stopped a \$6.9 million USD payment order originating with Defendants Credit Suisse in Zurich because the SWIFT-NET message details included the phrase "Bank Melli Iran."

1618. In fact, forty-four of the payments stopped by HSBC-US's OFAC filter in May 2005 alone (inadvertently) disclosed Iranian involvement.

1619. On June 3, 2005, HSBC-US informed Defendants HSBC Holdings that additional HSBC-London transfers in the amounts of \$1.9 million USD and \$160,000 USD had been

stopped by HSBC-US due to the lack of full disclosure of the originator, beneficiary, and purpose of the payment transaction.

1620. HSBC-London responded that both payment orders were foreign exchange related, the originators were Bank Tejarat and Bank Melli, and the beneficiaries of the USD funds were Persia International Bank and Defendants Credit Suisse's Zurich office, respectively.

1621. HSBC-US responded by requesting that HSBC-London follow up with the banks to obtain the names and addresses of the initial originators and ultimate beneficiaries, as well as confirmation of the underlying purpose of the payments.

1622. According to information provided by Bank Melli through HSBC-London, the \$160,000 payment denoted an internal transfer from Bank Melli's Eurodollar account with HSBC-London to Bank Melli's Eurodollar account with Defendants Credit Suisse's Zurich office.

1623. From July 2005 to June 2006, HBME sent more than 2,500 Iranian Eurodollar transactions – through its various SWIFT-NET network accounts for clearance and settlement by Defendants HSBC-US and/or other correspondent banks in the United States – that illegally concealed the required data relating to Iran.

1624. On November 23, 2005, in an email entitled "Cover payment processed to Credit Suisse re 'Bank Melli' – USD 100,000," an HSBC-US OFAC Compliance officer notified HSBC-London that, on November 7, 2005, a \$100,000 transaction involving Bank Melli had been processed through HSBC-London's USD account at HSBC-US without transparent documentation:

We are bringing this to your attention as this situation indicates that cover payment involving Iran are still being processed by PLC [referring to HSBC-London]. It was our understanding that Group payments involving Iran would be fully disclosed as to the originators and beneficiaries.

1625. In furtherance of the Conspiracy, from April 2006 through December 2007, about 50% of the estimated 700 Iranian Eurodollar payment transactions sent by HSBC-London—through its various SWIFT-NET network accounts for clearance and settlement by Defendants HSBC-US and/or other correspondent banks in the United States—continued to not disclose their connection to Iran.

1626. In addition, through March 2010, HSBC-US was the conduit for at least twenty-four post-U.S. designation Eurodollar transactions on behalf of IRISL and/or its various subsidiaries and front companies.

1627. HSBC-US's USD clearing and settlement operations with CHIPS-NY (Eurodollar clearing and settlement), CLS Bank (foreign exchange) and FRBNY (domestic USD clearing and settlement and central bank lender of last resort for the Eurodollar market) were being used by the HSBC Defendants to facilitate unlawful transactions in USD funds on behalf of Iran in furtherance of the Conspiracy.

1628. The DOJ issued a press release announcing the 2012 DPAs entry, including the fact the DPA resulted in HSBC Holdings and HSBC-US admitting to AML and sanctions violations, as well as the fact they would pay a \$1.256 billion USD forfeiture.

1629. In addition to the \$1.256 billion forfeiture under the DPA, HSBC Holdings and HSBC-US also agreed to pay \$665 million in civil penalties – \$500 million to the Comptroller of the Currency and \$165 million to the Federal Reserve – for the HSBC Defendants' AML and

combating the financing of terrorism program violations with Iran, other sanctioned countries, and transnational drug cartels.<sup>169</sup>

1630. The DOJ's press release announcing the DPA quoted then-Assistant Attorney General Lanny Breuer:

HSBC is being held accountable for stunning failures of oversight – and worse – that led the bank to permit narcotics traffickers and others to launder hundreds of millions of dollars through HSBC subsidiaries, and to facilitate hundreds of millions more in transactions with sanctioned countries. The record of dysfunction that prevailed at HSBC for many years was astonishing.

1631. Based on this and other illegal conduct by the HSBC Defendants on behalf of Iran and aimed at the United States financial system, HSBC Bank USA, N.A. and HSBC Holdings PLC chose to enter into sweeping DPAs with the United States DOJ and the United States Attorney's Office for the Eastern District of New York, the United States Attorney's office for the Northern District of West Virginia, and the New York County District Attorney's Office for willfully failing to maintain an effective AML program, in violation of Title 31 U.S.C. § 5318(h) and regulations issued thereunder; willfully failing to conduct and maintain due diligence on correspondent bank accounts held on behalf of foreign persons, in violation of Title 31 U.S.C. § 5318(i) and regulations issued thereunder; willfully violating and attempting to violate the Trading with the Enemy Act, Title 50 U.S.C., Appendix §§ 3, 5, 16, and regulations issued thereunder; and willfully violating and attempting to violate the IEEPA, Title 50 U.S.C. §§ 1702 and 1705, and regulations issued thereunder. In conjunction with these agreements, these HSBC defendants agreed the following facts are true and correct:

---

<sup>169</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Settlement Agreement entered into between the HSBC Defendants and the United States Department of Treasury on or about December 11, 2012, as if fully set forth herein.

- a) From the mid-1990s through at least September 2006, HSBC Group Affiliates violated both U.S. and New York State criminal laws by knowingly and willfully moving or permitting to be moved illegally hundreds of millions of dollars through the U.S. financial system on behalf of banks located in, *inter alia*, Iran, and persons listed as parties or jurisdictions sanctioned by OFAC in violation of U.S. economic sanctions. To hide these transactions, HSBC altered and routed payment messages in a manner that ensured that payments involving sanctioned countries and entities cleared without difficulty through HSBC Bank USA and other U.S. financial institutions in New York County and elsewhere.
- b) These HSBC defendants engaged in this conduct by knowingly:
  - i. following instructions from the Sanctioned Entities, including Iran, not to mention their names in USD payment messages sent to HSBC Bank USA and other financial institutions located in the United States;
  - ii. amending and reformatting USD payment messages to remove information identifying the Sanctioned Entities;
  - iii. using a less transparent method of payment messages, known as cover payments; specifically, HSBC used MT 202 cover payment messages for certain bank-to-bank credit transfers that resulted in USDs being made available for use in the terrorist attacks which killed or injured Plaintiffs. As a result of the HSBC Defendants' use of these improper MT 202 cover payment messages, U.S. financial institutions were unable to detect when payments were made to or from a sanctioned entity; and
  - iv. directly instructing its Iranian customers how to format payment messages in order to avoid bank sanctions filters that could have caused payments to be blocked or rejected.
- c) These HSBC defendants' conduct, caused HSBC Bank USA and other financial institutions located in the United States to process payments that otherwise should have been held for investigation, rejected, or blocked pursuant to U.S. sanctions regulations administered by OFAC.
- d) Additionally, by their conduct, these HSBC defendants:
  - i. prevented HSBC Bank USA and other financial institutions in the United States from filing required reports with the U.S. Government;
  - ii. caused false information to be recorded in the records of U.S. financial institutions located in New York, New York; and
  - iii. caused U.S. financial institutions not to make records they otherwise would have been required by law to make.

1632. As part of the Deferred Prosecution, HSBC Bank USA, N.A. and HSBC Holdings PLC expressly waived any challenges to the venue or jurisdiction and further agreed to, *inter alia*:

- a) Pay the United States \$1,256,000,000.00 in lieu of a forfeiture proceeding;
- b) Accept and acknowledge responsibility for its conduct and that of its employees, officers, directors, and agents, described above;
- c) Implement and/or continue to implement numerous changes to its corporate management, policies, and procedures;
- d) Cooperate fully with the DOJ in all investigations, including making available witnesses, documents, information, and other materials; and
- e) Maintain an independent compliance monitor.

1633. In September, 2012, the U.S. Senate's Permanent Subcommittee on Investigations issued a report regarding the HSBC Defendants entitled *U.S. Vulnerabilities to Money Laundering, Drugs, and Terrorist Financing: HSBC Case History* ("the HSBC Senate Report").<sup>170</sup>

1634. The HSBC Senate Report, which is over 300 pages, details the HSBC Defendants participation in the Conspiracy and their knowledge the USD funds they provided would be used to fund terrorist acts, including those perpetrated against plaintiffs.

1635. Some of the findings in the HSBC Senate Report include:

- a) "[F]or years, some HSBC affiliates took action to circumvent the OFAC filter when sending OFAC sensitive transactions through their USD correspondent accounts at HSBC-US [HSBC Bank USA N.A.]. From at least 2001 to 2007, two HSBC affiliates, HSBC Europe (HBEU) and HSBC Middle East (HBME), repeatedly sent U-turn transactions through HSBC-US without disclosing links to Iran, even though they knew HSBC-US required full transparency to process U-

---

<sup>170</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the HSBC Senate Report as if fully set forth herein.

turns. To avoid triggering the OFAC filter and an individualized review by HSBC-US, HBEU systematically altered transaction information to strip out any reference to Iran and characterized the transfers as between banks in approved jurisdictions. The affiliates' use of these practices, which even some within the bank viewed as deceptive, was repeatedly brought to the attention of HSBC Group Compliance, by HSBC-US compliance personnel and by HBEU personnel who objected to participating in the document alteration and twice announced deadlines to end the activity. Despite this information, HSBC Group Compliance did not take decisive action to stop the conduct or inform HSBC-US about the extent of the activity. At the same time, while some at HSBC-US claimed not to have known they were processing undisclosed Iranian transactions from HSBC affiliates, internal documents show key senior HSBC-US officials were informed as early as 2001. In addition, HSBC-US' OFAC filter repeatedly stopped Iranian transactions that should have been disclosed to HSBC-US by HSBC affiliates, but were not. Despite evidence of what was taking place, HSBC-US failed to get a full accounting of what its affiliates were doing or ensure all Iranian transactions sent by HSBC affiliates were stopped by the OFAC filter and reviewed to ensure they were OFAC compliant. . . . Other documents indicate that some HSBC affiliates may have sent non-USD messaging traffic through U.S. servers in which the OFAC filter was not turned on or was restricted."

- b) "An outside auditor hired by HSBC-US has so far identified, from 2001 to 2007, more than 28,000 undisclosed, OFAC sensitive transactions that were sent through HSBC-US involving \$19.7 billion. Of those 28,000 transactions, nearly 25,000 involved Iran, while 3,000 involved other prohibited countries or persons. The review has characterized nearly 2,600 of those transactions, including 79 involving Iran, and with total assets of more than \$367 million, as 'Transactions of Interest' requiring additional analysis to determine whether violations of U.S. law occurred."
- c) "[A]ctions taken by HSBC affiliates to circumvent OFAC safeguards may have facilitated transactions on behalf of terrorists, drug traffickers, or other wrongdoers. While HSBC-US insisted, when asked, that HSBC affiliates provide fully transparent transaction information, when it obtained evidence that some affiliates were acting to circumvent the OFAC filter, HSBC-US failed to take decisive action to confront those affiliates and put an end to the conduct. HSBC-US' experience demonstrates the strong measures that the U.S. affiliate of a global bank must take to prevent affiliates from circumventing OFAC prohibitions."
- d) **Disregarding Links to Terrorism.** For decades, HSBC has been one of the most active global banks in the Middle East, Asia, and Africa, despite being aware of the terrorist financing risks in those regions. . . . HSBC-US provided U.S. correspondent accounts to some foreign banks despite evidence of links to terrorist financing."

- e) “Documents collected by the Subcommittee do not pinpoint when undisclosed Iranian transactions began moving through HSBC-US in potential violation of OFAC regulations. HSBC officials were aware of the practice generally as early as 2000, as seen in an email discussion between HSBC Group’s Compliance head, then Matthew King, and AML head Susan Wright. Ms. Wright criticized actions taken by a bank client to alter transaction documentation to disguise a wire transfer moving through the United States, but their email exchange does not disclose whether such transactions were already taking place at HSBC-US. By 2001, they clearly were, as described in an email from HBEU to HSBC-US.”
- f) “From 2001 until 2005, the two HSBC affiliates [HBEU and HBME] frequently discussed processing Iranian USD transactions for various Iranian financial institutions and entities through their HSBC-US correspondent accounts. Numerous emails among HBEU, HBME, HSBC-US, and HSBC Group discuss whether HSBC-US would be willing to process Iranian U-turn transactions and, if so, how. At the same time, HSBC Group, HBEU and HBME bankers were pushing to expand contacts with Iran. The Senior Payments Manager in HSBC-US reported being told in a July 2001 conference call that the HSBC Group, with backing from the Chairman, was seeking to ‘significantly grow our presence in Iran.’ In 2003, an HBME business proposal estimated that processing 700 USD payments for Iranian banks per day using U-turn transactions would produce income of \$4 million, while failing to process them would threaten HSBC’s current Iranian business which produced annual bank income of \$2 million. HBME also noted that it already had a ‘number of existing USD accounts for Iranian banks.’” In 2001, an HBME compliance employee “cautioned that subjecting all OFAC sensitive payments to the OFAC filter for further review and approval would likely hurt business.”
- g) “At HSBC-US, during the same time period, internal documents show that, as early as 2001, senior HSBC-US payments, compliance, and business managers were informed that Iranian USD payments were being sent by HBEU through HSBC-US after deleting references to Iran. They were also informed of an HBEU proposal to streamline the processing of U-turn transactions by omitting references to Iran so the transactions would not be halted by the OFAC filter in the United States. Emails at the time show that senior HSBC-US officials expressed discomfort with the HBEU proposal, but took no other action to stop or prevent the activity already occurring. In addition, HSBC-US’ OFAC filter occasionally caught an Iranian-related transaction, sent by an HSBC affiliate, in which the identifying information had not been fully removed, demonstrating that undisclosed U-turns continued to be sent through HSBC-US correspondent accounts, but again, no HSBC-US personnel took further action to stop the activity. In 2003, the Iranian issue was discussed again when a new HSBC-US AML Director arrived, but once more, no decisive action was taken to put a stop to undisclosed U-turns.”
- h) “Although HSBC Group Compliance was aware of HSBC-US’ concerns, HBEU’s practice of stripping information or using cover payments to conceal U-

turn transactions involving Iran, and the fact such undisclosed transactions were routinely slipping through HSBC-US accounts, HSBC Group did not prohibit the practice for years.”

- i) “In 2010, HSBC Group employed an outside auditor, Deloitte LLP, to identify and review OFAC sensitive transactions at HSBC-US over a seven-year period from 2001 to 2007. That review has so far examined 58 million payment messages involving assets of \$37 billion that passed through the key server, located in the United Kingdom, during that timeframe and identified OFAC sensitive USD transactions involving assets totaling \$19.7 billion. The review identified almost 25,000 USD transactions involving Iran, involving assets in excess of \$19.4 billion. The vast majority of the Iranian transactions, ranging from 75% to 90% over the years, were sent through HSBC-US and other USD accounts without disclosing any connection to Iran. . . . [I]n 2003, HSBC affiliates sent at least 5,400 Iranian transactions to USD accounts in the United States, of which about 90% were not disclosed. . . . According to an ongoing outside audit requested by HSBC, from 2001 to 2007, HBEU and HBME sent through their USD accounts at HSBC-US and elsewhere nearly 25,000 OFAC sensitive transactions involving Iran totaling \$19.4 billion. While some of those transactions were fully disclosed, most were not. According to the review conducted by Deloitte, from April 2002 to December 2007, more than 85% of those payments were undisclosed.”
- j) In connection with the HSBC Defendants’ OFAC violations regarding the Bank Melli, in 2001, Douglas Stolberg, head of HSBC-US Commercial and Institutional Banking (CIB), wrote to HSBC compliance personnel: “With the amount of smoke coming off of this gun, remind me again why we think we should be supporting this business?”
- k) In August, 2001, an HSBC memorandum stated that “it is estimated that Iranian banks issue up to 700 USD payments a day using their USD service providers, mainly banks in the UK and Europe, which in turn use their New York USD correspondents to effect [sic] the payments. It is believed that some service providers amend the payments to ensure Iran is not mentioned in the body of the payment instruction to their USD correspondent. This process minimizes the risk of payment being referred to OFAC.” The memo further stated that “there is a substantial income opportunity to see a USD payments proposition to Iranian Banks.”
- l) In an October, 2003 HSBC paper entitled “Iran – Strategy Discussion Paper,” the company “listed ‘significant business wins’ involving Iran, in the Project and Export Finance, Trade Finance, and Treasury and Capital Markets areas with an estimated \$7 million per year in revenues generated by Iranian businesses for ‘various Group entities.’ In a section entitled, ‘Phase 1 – Immediate Opportunities,’ the strategy stated that Iran’s annual international trade business was valued at \$25 billion, 80% of which was denominated in USD. It stated that HBEU [Payment and Cash Management] currently offered USD payment services

to four Iranian banks, and could market the same services ‘to other Iranian commercial banks, including Iran’s Central Bank (Bank Markazi).’ It estimated the potential business as worth up to \$4 million per year.”

- m) In July, 2004, an HBEU proposal noted that “Bank Melli, Bank Markazi, Bank Tejarat, Bank Kesharvazi, and the Export Development Bank of Iran were the five Iranian financial institutions that took advantage of [H SBC’s] practice to effect USD payments with a daily volume estimated at between 10 and 50 payments per day at an approximate total value of \$500,000 to \$1 million. The proposal also noted the Central Bank payments were much larger, in the range of \$10 million, and were typically made at certain times of the month.” Around that time, an HSBC employee “characterized the risks associated with the existing practice as including operational losses due to payment seizure, threats to HSBC’s reputation, and ‘incurring hefty fines.’” He explained that ‘few if any U.K. banks are in the business.’”
- n) “[O]ne . . . notable transaction involving Iran in 2006[] pertained to 32,000 ounces of gold bullion valued at \$20 million. In May 2006, the HSBC-US London branch cleared the sale of the gold bullion between two foreign banks for the ultimate benefit of Bank Markazi, Iran’s Central Bank. HSBC indicated that it had been aware that Bank Markazi was the beneficiary, but had viewed the transaction as a permissible Uturn.”
- o) An October, 2006 email to the HSBC Group Chairman, HSBC Group CEO, and the HSBC Group COO informed them that elements in the Bush administration “were in favour of withdrawing the U-turn exemption from all Iranian banks. This on the basis that, whilst having direct evidence against Bank Saderat particularly in relation to the alleged funding of Hezbollah, they suspected all major Iranian State owned banks of involvement in terrorist funding and WMD [weapons of mass destruction] procurement.”
- p) “The subject of Iran arose again a few months later, in June 2007, when Mr. Bagley [head of HSBC Group Compliance] informed HSBC Group CEO Michael Geoghegan that he had a private meeting with U.S. Treasury Under Secretary for Counter Terrorist Financing and Sanctions, Stuart Levey, during a recent Wolfsberg Group conference. Mr. Bagley indicated that Mr. Levey had questioned him about a HSBC client who, according to Mr. Levey, ‘had clearly been identified as having acted as a conduit for Iranian funding of’ an entity whose name was redacted from the document by HSBC. Mr. Bagley wrote: ‘Levey essentially threatened that if HSBC did not withdraw from relationships with [redacted] we may well make ourselves a target for action in the US.’ Mr. Geoghegan responded: ‘This is not clear to me because some time ago I said to close this relationship other than for previously contractually committed export finance commitments.’ Mr. Bagley replied that the bank had only ‘limited relationships with [redacted] and in fact overall with Iranian banks.’”

- q) “[I]nternal bank documents show that hundreds of Iranian transactions per month continued to surface at HSBC-US during 2008 and 2009. . . . In 2008 and 2009, for example, HSBC-US’ London Banknotes office conducted a series of apparently prohibited transactions benefitting the Iranian Embassy in London. From July 22, 2008 to February 12, 2009, in more than 30 transactions, HSBC-US sold over €455,000 to HBEU which, in turn, sold them to the Embassy of Iran in the United Kingdom. According to HSBC-US, ‘the funds were used to meet salary obligations’ of the Iranian Embassy. In addition from December 5, 2008 to February 5, 2009, HBEU purchased over \$2,500 from the Embassy of Iran and resold the USDs to HSBC-US. . . . Other transactions involving Iran processed through HSBC-US’ correspondent accounts from 2008 to 2009, included a March 2009 wire transfer for \$300,000, which was mistakenly processed because a HSBC-US compliance officer did not realize a transaction reference to ‘Persia’ implied a connection to Iran; and two wire transfers totaling over \$55,000 which involved a vessel owned by ‘NITC’ which, until it was updated, HSBC-US’ OFAC filter did not recognize as the National Iranian Tanker Company.”
- r) “Despite HSBC-US pleas for transparency and a 2004 internal agreement to use fully transparent procedures, HSBC affiliates HBEU and HBME often took action, including by deleting references to Iran or using cover payments, to prevent the Iranian transactions sent through their USD correspondent accounts at HSBC-US from being caught in the OFAC filter. Despite the fact they viewed most of the transactions as permissible under U.S. law, concealing their Iranian origins helped avoid delays caused when HSBC-US’ OFAC filter stopped the transactions for individualized review. HBME, in particular, requested that HSBC-US allow the use of cover payments to conceal Iranian transactions and circumvent the OFAC filter. When HSBC-US insisted on fully transparent transactions, the HSBC affiliates sent undisclosed transactions through their HSBC-US accounts anyway. HSBC Group leadership, including the heads of Compliance and AML, were aware in varying degrees of what the affiliates were doing, but for years, took no steps to insure HSBC-US was fully informed about the risks it was incurring or to stop the conduct that even some within the bank viewed as deceptive. The HSBC Group Compliance head took no decisive action even after noting that the practices ‘may constitute a breach’ of U.S. sanctions. At HSBC-US, senior executives in the Compliance and payments areas knew about the actions being taken by HSBC affiliates to send concealed Iranian transactions through their USD correspondent accounts, but were unable or unwilling to obtain information on the full scope of the problem, bring the issue to a head, and demand its resolution at the highest levels of the bank to ensure all U-turns were reviewed for compliance with the law.”
- s) “In addition to transactions involving jurisdictions subject to U.S. sanctions programs, some transactions sent to HSBC-US involved prohibited individuals or entities named on the OFAC SDN list. While many of these transactions were not sent by HSBC affiliates, some were. HSBC-US did not allow such transactions to proceed, showing the effectiveness of the OFAC filter when all appropriate transactions are run through it.”

- t) “On November 9, 2006, for example, ‘at the direction of OFAC,’ HSBC-US blocked for further review a \$32,000 payment that had been originated by HBME, because the underlying payment details indicated the funds were to be credited to Al Aqsa Islamic Bank. This bank had been designated as a ‘specially designated global terrorist’ by OFAC in December 2001, because it was a ‘direct arm of Hamas, established and used to do Hamas business.’ On November 20, 2006, HBME asked HSBC-US to cancel the payment, because ‘it was sent in error.’ On December 7, 2006, however, OFAC instructed HSBC-US to continue to block the funds. HSBC-US AML Compliance head Teresa Pesce wrote: ‘How is it that these payments continue to be processed by our affiliates in light of the [Group Circulation Letter] GCLs?’
- u) “A report prepared by Deloitte at HSBC-US’ request, examining the period 2001 to 2007, also disclosed that one USD correspondent account located in the United Kingdom had been opened for a bank located in Syria, while two USD correspondent accounts in the United Kingdom had been established for the ‘Taliban.’ When asked about the correspondent account for a bank established for the Taliban, HSBC legal counsel told the Subcommittee that HBEU had maintained an account for Afghan National Credit and Finance Limited, the London subsidiary of an Afghan bank that, from October 22, 1999 to February 2, 2002, was designated under OFAC’s Taliban sanctions 1015. An HSBC-US representative told the Subcommittee that HSBC-US was unable to go back far enough in its records to uncover whether or not the Afghan account at HBEU sent transactions through HSBC-US during that time. The fact HBEU had this account after the 9/11 terrorist attack on the United States again demonstrates how HSBC affiliates took on high risk accounts that exposed the U.S. financial system to money laundering and terrorist financing risks. These USD accounts may also have contravened the 2005 GCL and OFAC regulations by enabling banks in Syria and Afghanistan when it was controlled by the Taliban to engage in USD transactions through HSBC-US.”
- v) “OFAC enforces U.S. programs aimed at exposing and disabling the financial dealings and resources of some of the most dangerous persons and jurisdictions threatening the world today, including terrorists, persons involved with weapons of mass destruction, drug traffickers, and rogue jurisdictions. The OFAC filter is the central mechanism used to identify, stop, and block suspect transactions speeding through financial systems. Global financial institutions have a special responsibility to respect OFAC prohibitions and comply with OFAC restrictions. actions taken to circumvent the OFAC filter or endanger the effectiveness of a critical safeguard may facilitate transactions undertaken by some of the worst wrongdoers among us.”
- w) “The evidence reviewed by the Subcommittee indicates that, from 2001 to 2007, HSBC affiliates, with the knowledge and tacit approval of HSBC Group executives, engaged in alarming conduct sending undisclosed Iranian U-turn transactions through their HSBC-US correspondent accounts, without information that would otherwise have triggered OFAC reviews. When asked, HSBC-US

insisted on HSBC affiliates using transparent payment instructions so that all U-turn transactions would be stopped by the OFAC filter and reviewed, but when faced with evidence that some HSBC affiliates were acting to circumvent the OFAC filter, HSBC-US failed to take decisive action to stop the conduct some in its own organization viewed as deceptive. In addition, from at least 2009 to early 2012, the bank's OFAC compliance program suffered from multiple deficiencies. Still another issue is that some HSBC affiliates sent non-USD messaging traffic through U.S. servers in which the OFAC screening was not turned on or was restricted. The aim in many of the instances in which HSBC affiliates acted to circumvent the OFAC filter may have been to avoid the time-consuming individualized reviews that followed, rather than execute prohibited transactions. But expediency in the face of the threats posed by the targets of OFAC prohibitions does not justify potentially violating or undermining OFAC requirements. HSBC-US likewise failed to obtain information about the full scope of undisclosed OFAC sensitive transactions going through its correspondent accounts, bring to a head the issue of HSBC affiliates circumventing OFAC safeguards, and ensure all transactions were reviewed for OFAC compliance.”

1636. In sum, the HSBC Senate Report as well as related Deferred Prosecution Agreement, HSBC employee emails, and SWIFT-NET payment order messages evince the HSBC Defendants intentionally violated U.S. sanctions in providing USD, expert advice, financial services, and financial securities to Iranian entities, knowing the USD would be used by Terrorist Groups, to carry out the Terrorist Attacks, as well as other acts of international terrorism.

#### **4. Commerzbank's Participation in the Conspiracy**

1637. Since 1967, Commerzbank has had a license issued by the State of New York to operate within that state as a foreign bank. Commerzbank has operated a branch in New York City since that time, known as Commerzbank New York.

1638. Among its primary function, Commerzbank New York serves as the clearing house for international USD transactions for Commerzbank's variety of international clientele.

1639. From approximately 2002 through 2008, Commerzbank systematically and continuously violated United States and New York law by conducting prohibited USD

transactions by artfully and intentionally disguising such transactions to avoid detection by United States and New York regulators.

1640. In particular, Commerzbank knowingly and intentionally concealed from United States and New York financial institutions (including its own), regulators and law enforcement officials, the fact it was processing USD payments for sanctioned Iranian entities. Based on this conduct, United States financial institutions, regulators and law enforcement were not able to block, stop, or investigate hundreds of millions of dollars in USD transactions perfected in favor of sanctioned Iranian entities.

1641. Beginning by at least 2002 and continuing through at least 2008, Commerzbank had a continuous, ongoing relationship with Iran and its Agents and Proxies.

1642. From 2002 to 2008, Commerzbank knowingly and willfully moved \$253 billion through the U.S. financial system on behalf of Iranian and Sudanese entities subject to U.S. economic sanctions. Commerzbank engaged in this criminal conduct using numerous schemes designed to conceal the true nature of the illicit transactions from U.S. regulators.<sup>171</sup>

1643. As noted in a criminal information entered in connection with, as discussed below, a March 11, 2015 DPA between Defendants Commerzbank and DOJ:

COMMERZBANK AG and others ... unlawfully, willfully and knowingly combined, conspired, confederated and agreed with one another and with others to commit offenses against the United States, that is, to engage in financial transactions with Sanctioned Entities and SDNs in violation of IEEPA, and the executive orders and regulations issued thereunder.... The goal of the conspiracy was for COMMERZBANK and others ...to enrich themselves by engaging in a conspiracy and a scheme to violate IEEPA, and the executive orders and regulations issued thereunder. A further goal of the conspiracy was for COMMERZBANK and others ... to violate executive orders and regulations

---

<sup>171</sup> New York State Department of Financial Services, *In re Commerzbank AG, Commerzbank AG New York Branch, Consent Order Under New York Banking Law §§ 39 and 44*, <http://www.dfs.ny.gov/about/ea/ea150312.pdf> (last visited Oct. 15, 2017).

prohibiting the exportation, directly and indirectly, of services from the United States to Sanctioned Entities and SDNs.<sup>172</sup>

1644. Like many of the other Defendants who entered into the Conspiracy, Commerzbank adopted a variety of methods to facilitate Iran's illegal goals.

1645. In particular, Commerzbank worked with Bank Sepah, Bank Melli, Bank Saderat and Bank Refah to facilitate the goals of the Conspiracy, stripping, altering, or changing tens of thousands of SWIFT-NET payment order messages.

1646. Since 2002, Commerzbank also appears to have engaged in various illegal gold transactions on behalf of the CBI, including trading orders through its New York branch while disguising the Iranian source of the trades.

1647. A March 2015 Amended Complaint filed in a *qui tam* case against Defendants Commerzbank AG stated:

the gold trade has been essential to Iran's withstanding the increasingly restrictive U.S. sanctions. It has a substantial amount of gold reserves, amounting to \$112 billion in gold, which it accumulated in part by trading oil for gold. It used gold to preserve its wealth especially to withstand the devaluation of its currency and to engage in trading that would bypass U.S. sanctions.

1648. On April 17, 2003, Commerzbank finalized a policy document entitled "Routing Instructions Iranian banks for USD payments." This policy admonished employees to "[u]nder no circumstances mention the Iranian background in the cover order." In other words, the German-based recipients of this policy were instructed to never mention Iranian customers nor Iranian connections to any payment messages sent to the United States.

1649. Taking advantage of the fact Lloyds and other competitors were exiting the Iranian market, Commerzbank solicited more Iranian clients.

---

<sup>172</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPA entered into between Commerzbank and the DOJ on or about March 11, 2015, as if fully set forth herein.

1650. The resulting increase in the volume and significance of Iranian business at Commerzbank led to the establishment of a centralized process for handling certain Iranian dollar denominated payments within Commerzbank, and Defendants designated one group of employees within Commerzbank's Frankfurt Back Office to manually process those payments.

1651. The task of this group was to review payments and amend them if necessary, to ensure they would not get stopped by OFAC filters when sent to financial institutions in the United States, including Commerzbank's New York branch.

1652. This increase in volume was in part due to illicit trade-finance, foreign exchange, and Eurodollar transactions undertaken by Commerzbank on behalf of Bank Refah, Bank Sepah, Bank Melli, and Bank Saderat.

1653. In July 2003, a back-office employee emailed other bank employees explaining that two state-owned Iranian banks, Bank Melli and Bank Saderat, wanted to begin routing their entire USD funds clearing business through Commerzbank. The back-office employee closed his email by writing, "If for whatever reason [Commerzbank] New York inquires why our turnover has increase[d] so dramatically under no circumstances may anyone mention that there is a connection to the clearing of Iranian banks!!!!!!!!!!!!!"

1654. On September 17, 2003, a back-office employee sent an email advising a major Iranian Bank that maintained a US dollar account with Commerzbank to list "non ref" in the ordering party field in all of its future payment messages.

1655. The author of the email had tested Commerzbank's compliance systems in Frankfurt, and knew that writing "non ref" would trigger a manual review of the payment, thereby enabling Commerzbank personnel to ensure the messages did not contain any information revealing the true Iranian involvement in the transaction.

1656. In fact, Commerzbank personnel explained to employees of Iranian bank clients the kinds of information that could lead to payments being delayed, rejected, or blocked within the United States, and encouraged the Iranian banks to omit this type of information from their payment orders so that Commerzbank employees would not have to manually remove it.

1657. For example, Bank Sepah's UK subsidiary (Bank Sepah International Plc) provided its Iranian customers with routing instructions for "payments to our US Dollar account from outside the United States" noting the SWIFT Code for Commerzbank's New York branch and the Bank's account number at Commerzbank followed by the instruction: "**Please ensure that no mention is made of any recognisable Iranian entity in any message sent through the United States.**" (emphasis in the original).

1658. On October 13, 2003, the Head of Commerzbank's Internal Audit division emailed a member of Commerzbank's senior management advising that Iranian bank names in payment messages transiting through the United States were being "neutralized" and warned that "it raises concerns if we consciously reference the suppression of the ordering party in our work procedures in order to avoid difficulties in the processing of payments with the U.S.A."

1659. On November 19, 2003, a memo was circulated to senior management memorializing the internal rules Commerzbank had developed for processing Iranian payments, including using MT 202 cover transactions (i.e., splitting a payment into two messages and sending a MT 103 to the foreign (non-U.S.) branch of the beneficiary and an MT 202 to the clearing institution in the United States), and using serial MT 103 messages that manually replaced the name of the (Iranian) ordering party with the bank code for Commerzbank Frankfurt to avoid detection by U.S. authorities.

1660. It appears that Commerzbank may have ceased stripping some transactions in July 2004, relying primarily on cover payments (MT 202 payment order messages) to effectuate its unlawful conduct. At the same time, Commerzbank conspired with Bank Melli to facilitate over one hundred (100) checks totaling approximately \$2 million in USD funds that Commerzbank issued for illegal payments in the United States.

1661. However, as noted *supra*, Bank Sepah International Plc (Bank Sepah's UK subsidiary) provided "stripping" instructions to its clients even in 2006 directing that USD wire transfers be sent through Commerzbank's New York branch.

1662. DOJ described "the rigor with which the Bank enforced the policy during this period" by citing an email from an employee who wrote about Commerzbank's procedures for facilitating the Conspiracy "NO EXPERIMENTS PLEASE!!! Have fun with this and greetings."

1663. This ongoing conduct involving both "stripping" transactions and converting otherwise transparent SWIFT-NET MT 103 messages into opaque MT 202 cover transactions resulted in tens of millions of dollars being illegally transferred on Iran's behalf.

1664. However, parallel to its illegal conduct on behalf of Bank Sepah, Bank Saderat, and Bank Melli, as noted above, Commerzbank also directly coordinated with IRISL in laundering USD through the United States despite the fact IRISL was Iran's primary means of transporting both conventional and non-conventional weapons.

1665. Between 2002 and 2008 (and upon information and belief, even later), Commerzbank worked directly with IRISL to facilitate illicit payments through the United States.

1666. In January 2005, Commerzbank's New York branch rejected a series of payment transactions on behalf of Lancelin Shipping Company Ltd., an IRISL-formed entity registered in

Cyprus, because the payment messages contained references to IRISL Europe GmbH, a wholly-owned IRISL subsidiary registered in Hamburg and designated by the United States in 2008.

1667. This prompted a direct meeting between the relationship managers in Commerzbank's Hamburg branch and employees from IRISL on January 24, 2005.

1668. A memorandum summarizing the meeting noted that: “[d]ue to the tense political relations between Iran and the U.S., sanctions that have existed for some years against Iran and Iranian companies have been tightened.... *The number of rejected payments recently increased sharply since the word “IRISL” results in inquiries at foreign banks.* Based on inquiries from Commerzbank, New York we assume that it appears as a term on the embargo list.” (emphasis in the original).

1669. In a written presentation that Commerzbank delivered to IRISL on January 25, 2005, following the in-person meeting, the Hamburg relationship manager stated: “[t]he current rejections show that IRISL is in the OFAC list” (emphasis in the original).

1670. The presentation then explained that “payments which are sent through a ... subsidiary are unlikely to be rejected to our present knowledge.”

1671. Commerzbank ultimately adopted a process it termed a “safe payments solution” by which IRISL initiated USD funds transfers through the U.S., using the accounts of less conspicuous subsidiaries to prevent its New York branch or other clearing banks from flagging IRISL USD transactions.

1672. Moreover, to assist IRISL in its bookkeeping, Commerzbank would sweep those accounts daily and zero them out so that IRISL could keep track of which USD funds belonged to it – as opposed to its subsidiaries.

1673. On April 18, 2006, Commerzbank's New York branch rejected a payment on behalf of Lancelin, citing "US sanctions against Iran." As a result, Commerzbank altered the structure of the "safe payment solution," suggesting the use of two other subsidiaries to process payments on behalf of IRISL and IRISL Europe GmbH.

1674. In fact, in only four months following IRISL's U.S. designation in 2008, Commerzbank illegally transferred almost \$40 million on behalf of IRISL subsidiaries and related entities through Commerzbank's New York branch and other U.S. financial institutions.

1675. These post-designation transactions, laundered by Commerzbank through the U.S. financial system, were self-evidently not for the benefit of a legitimate agency, operation or program of Iran.

1676. Only months earlier, a U.S. State Department diplomatic cable warned of an IRISL-flagged vessel in China loaded with cargo containing weapons for Iran's DIO.

1677. The 2008 diplomatic cable further warned of the dangers of ongoing conventional arms transfers from China to Iran, "particularly given Iran's clear policy of providing arms and other support to Iraqi insurgents and terrorist groups like the Taliban and Hezbollah.... We have specific information that Chinese weapons and components for weapons transferred to Iran are being used against U.S. and Coalition Forces in Iraq, which is a grave U.S. concern."

1678. Less than a year after Commerzbank in Hamburg provided IRISL with at least \$40 million in illegal (post-designation) USD transactions in October 2009, U.S. troops boarded a German-owned freighter, the Hansa India, in the Gulf of Suez and found eight containers full of ammunition, and headed to Syria from Iran.

1679. The Hansa India was registered to the Hamburg-based shipping company Leonhardt & Blumberg, but had in fact been under charter to IRISL for several years.

1680. The Hansa India carried seven containers of small arms ammunition, as well as one container containing copper discs, which constitute, as noted *supra*, a key component in EFPs used to kill and maim many of the Plaintiffs herein.

1681. Although Commerzbank worked to shield its New York branch from knowing all of the details of its illicit activities on behalf of Iran and IRISL, Commerzbank's New York branch was nonetheless aware that it was being used to facilitate unlawful conduct.

1682. For example, in June 2006, in response to a request from the new Chief Compliance Officer asking if there were any concerns they wanted her to share with the new Global Head of Compliance in Germany, a New York compliance employee responded “[p]ersistent disregarding of OFAC rules by foreign branches. Hamburg is notorious for it.”

1683. In February 2007, Commerzbank's then Chief Executive Officer Klaus-Peter Mueller and Board Member Martin Blessing met with U.S. Treasury Deputy Secretary Robert Kimmitt. In the meeting, Mueller complained about the portrayal of Commerzbank by The Wall Street Journal (in a January 2007 article) which he said made it appear the Bank was trying to evade sanctions on Iran. “This,” claimed Mueller “is far from the case.”

1684. The Wall Street Journal reported on January 10, 2007 that “Commerzbank AG, Germany's second largest bank, said it will stop handling dollar transactions for Iran at its New York branch by Jan. 31.” It went on to report that “[a]t present, Commerzbank handles both dollar and euro transactions for Iran's state owned banks. Like several other European banks, it will cease handling only dollar transactions.”

1685. The Wall Street Journal article went on to report:

The risks of doing business with Iran are the same in all currencies,” said Mr. [Stuart] Levey. Intelligence officials say Bank Saderat, a large, state-controlled Iranian bank placed on a U.S. Treasury blacklist in October for allegedly funding terrorism, has been able to process dollar transactions through Commerzbank's

New York branch in recent months by using the accounts of two other Iranian banks. Commerzbank says it ceased dealing with Saderat after it was put on the U.S. blacklist and has no knowledge of any subsequent transactions. “Commerzbank has no knowledge of Bank Saderat directly or indirectly using the accounts of other Iranian banks to process dollar transactions,” the bank said in a statement. Commerzbank, in a response to an inquiry from The Wall Street Journal about its dealings with Iran, also said “all such [dollar clearing] transactions are currently being phased out” as of Jan. 31. It added that “any clearing conducted by our U.S. operations is in strict compliance” with U.S. government regulations.

1686. Commerzbank’s assurances to The Wall Street Journal, like its assurances to U.S. Treasury Deputy Secretary Robert Kimmitt, were plainly false.

1687. As noted above, on September 10, 2008, the U.S. designated IRISL, IRISL Europe GmbH, and several IRISL subsidiaries based on evidence the IRISL network of companies was engaged in WMD proliferation activity and the fact “IRISL has pursued new strategies which could afford it the potential to evade future detection of military shipments.”

1688. The next day, on September 11, 2008, a senior official at OFAC personally forwarded the press release announcing IRISL’s SDN designation to the Head of Compliance at Commerzbank in New York.

1689. The press release was then forwarded to Commerzbank employees in Germany with responsibilities related to IRISL. In the email, the relationship manager noted the U.S. government alleged “that IRISL as Iranian government carrier systematically circumvents the Iranian arms embargo.”

1690. Nonetheless, between September 10, 2008, and December 31, 2008 alone, Commerzbank illegally directed close to \$40 million on behalf of IRISL subsidiaries and related entities through the United States.

1691. During this same time period, Commerzbank also knowingly, or with deliberate indifference to the fact, maintained account number 7001688 for an open and notorious

Hezbollah fundraising organization in Germany known as Waisenkinderprojekt Libanon e.V. (“the Orphans Project Lebanon e.V.”).

1692. Despite prior public German government reports identifying its customer as a Hezbollah fundraising organization, and the fact on July 24, 2007 the United States designated the Lebanese organization that was primary recipient of funds donated from the account (Hezbollah’s Martyrs Foundation), Commerzbank knowingly, or with deliberate indifference to the fact, continued to provide financial services to Waisenkinderprojekt Libanon e.V. and hence continued to transfer funds to Hezbollah.

1693. Commerzbank used non-transparent payment messages, known as cover payments, to conceal the involvement of sanctioned entities, and also removed information identifying sanctioned entities from payment messages, in transactions processed through Commerzbank New York and other financial institutions in the United States. Specifically, in 2003, Commerzbank designated a group of employees in the Frankfurt back office to review and amend Iranian payments so the payments would not be stopped by U.S. sanctions filters. In doing so, Commerzbank ensured that Iranian payment messages did not mention the Iranian entity, as transactions may have otherwise been stopped pursuant to the U.S. sanctions.

1694. Commerzbank hid these practices from Commerzbank New York. For example, in 2003, when two state-owned Iranian banks wanted to begin routing their USD clearing business through Commerzbank, a Commerzbank back office employee emailed other Commerzbank employees directing: “If for whatever reason CB New York inquires why our turnover has increase[d] so dramatically, under no circumstances may anyone mention that there is a connection to the clearing of Iranian banks!!!!!!!!!!!!!!.”

1695. Commerzbank's conduct continued even though its senior management was warned the bank's practices for Iranian clients "raised concerns." For example, in October 2003, the head of Commerzbank's internal audit division stated in an email to a member of Commerzbank's senior management that Iranian bank names in payment messages going to the United States were being "neutralized" and warned: "it raises concerns if we consciously reference the suppression of the ordering party in our work procedures in order to avoid difficulties in the processing of payments with the U.S.A."

1696. In another scheme designed to avoid U.S. sanctions, Commerzbank admitted that, in 2004, it agreed with an Iranian bank client that, rather than sending direct wire payments to the United States, the Iranian bank would pay U.S. beneficiaries with Commerzbank-issued checks listing only the Iranian bank's account number and address in London with no mention of the Iranian bank's name.

1697. Additionally, Commerzbank admitted that in 2005, it created a "safe payment solution" for an Iranian shipping company client, which allowed the client to conduct transactions using the U.S. financial system. The safe payment solution involved routing payments through special purpose entities controlled by the Iranian company, which were incorporated outside of Iran and bore no obvious connection to the Iranian client. Commerzbank and its client switched use of such special purpose entities when Commerzbank New York's sanctions compliance filters were updated to detect the use of a particular special purpose entity. Commerzbank continued to process payments on behalf of the Iranian client even after the client had been designated by OFAC as an entity subject to U.S. sanctions for its involvement in WMDs proliferation.

1698. Based on this conduct and other illegal money laundering conduct in favor of Iran, Commerzbank entered into a DPA with the United States DOJ based on a four-count criminal information filed, accusing Commerzbank of violating the IEEPA (18 U.S.C. § 371), the Bank Secrecy Act (31 U.S.C. §§ 5318, 5322, failing to report suspicious activity under 31 U.S.C. §§ 5318, 5322, and failing to establish due diligence for foreign correspondent accounts in violation of 31 U.S.C. §§ 5318, 5322.

1699. Also based on this conduct, Commerzbank entered into a consent order with the DFS for violations of 3 N.R.C.R.R. § 116.2 for failing to maintain an effective and compliant money laundering/OFAC compliance program, New York Banking Law § 200-c for failing to maintain accurate books and records and 3 N.R.C.R.R. § 3.1 for knowingly making false entries and intentional omissions from its financial records keeping with the intent to deceive United States and New York regulators.<sup>173</sup>

1700. Further, Commerzbank entered into a Settlement Agreement with OFAC for, among other violations, violating 31 C.F.R. § 560.204 prohibiting the exportation or re-exportation of services from the United States to Iran.<sup>174</sup>

1701. Commerzbank agreed to pay a fine of \$79,000,000 dollars and forfeit \$560,000,000 to the United States based on this conduct. Commerzbank also agreed to separately pay \$610,000,000 as a civil penalty in resolution of the action brought by New York State. Commerzbank was also assessed \$258,660,796 as a contingent fine by the United States

---

<sup>173</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order entered into between Commerzbank the New York Department of Financial Services on or about March 12, 2015, as if fully set forth herein.

<sup>174</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Settlement Agreement entered into between Commerzbank the United States Department of Treasury on or about March 12, 2015, as if fully set forth herein.

Department of the Treasury in the event the financial penalties from settlements with other governmental entities did not meet that amount.

1702. Agreeing to the factual predicate for these offenses, Commerzbank admitted to widespread, consistent, and illegal conduct laundering money for Iran, Iranian banks, and other Iranian entities, including:

- a) From approximately 2002 through 2008, Commerzbank assisted Iran and Iranian entities in facilitating USD transactions despite the fact these entities were barred under OFAC regulations and other applicable laws.
- b) As a result of this facilitation, Commerzbank New York and other United States financial institutions processed hundreds of millions of dollars in USD transactions for sanctioned entities tied to Iran that should otherwise have been rejected, blocked or investigated.
- c) Specifically, these actions by Commerzbank caused (1) untold number of illegal transactions from being detected by United States and New York regulatory and law enforcement agencies; (2) prevented United States financial institutions, including Commerzbank New York, from filing sanction-related reports with the United States government; (3) false entries to be recorded in the business records of United States and New York financial institutions, and (4) United States and New York financial institutions to not create records that should have otherwise been created, as required by United States and New York law, but for the fraudulent concealment.

1703. The following are a selection of specific examples of Commerzbank's conduct that allowed Iran and Iranian entities to clear hundreds of millions of dollars in USD transactions:

- a) Commerzbank's branch in Frankfurt developed a systemic practice of using cover payments for Iranian entities that would effectively eliminate OFAC filters implemented by the Commerzbank New York branch designed to root out transactions with such sanctioned entities.
- b) As early as 2003, Commerzbank had a specific policy in place for routing instructions for Iranian banks that included the admonition "under no circumstances mention the Iranian background in the cover order." Commerzbank internally stated the basis for this rule is that "there is a high risk that transactions and cover payments with Iranian Background via USD might be blocked." This information and practice was not shared with Commerzbank New York and had

the intended effect of preventing detection of prohibited transactions by United States and New York regulators.

- c) Later in 2003, many European banks decided to do USD transaction business with Iranian entities no longer, specifically because of the United States sanctions in place. Commerzbank viewed this as a business opportunity to fill a void left by law abiding banks and took on significant USD clearing business for several Iranian banks and entities.
- d) In fact, Commerzbank went as far as to set up a specialized group overseeing a centralized process in Frankfurt by which Iranian entity USD payment requests were reviewed and amended, if necessary, to ensure they would not get caught in OFAC filters maintained at the Commerzbank New York branch.
- e) This specialized group issued specific instructions to keep the fact they were processing USD transactions for Iranian-owned Bank Melli, Bank Sepah and Bank Saderat a secret. In addressing the uptick in USD clearance payments through the Commerzbank New York branch, this group instructed “[i]f for whatever reason CB New York inquires why our turnover has increase [sic] so dramatically under no circumstances may anyone mention that there is a connection to the clearing of Iranian banks!!!”
- f) In addition to implementing its own policies to have the Iranian USD transaction hidden from United States and New York regulators, Commerzbank instructed the Iranian entities on how to best assist them in avoiding detection by these regulators. By instructing the Iranian banks to put “non ref” in the ordering party field, this would trigger the Commerzbank Frankfurt employees to manually review the payment to ensure all Iranian-identifying information was cleaned from the payment request.
- g) Commerzbank also provided other detailed information to Iranian entities on what type of information would cause USD payments to be blocked, rejected or investigated so they could avoid including that type of information in requested USD transactions.
- h) As early as 2003, Commerzbank employees were presenting senior management with options to avoid detection of Iranian entity payments by United States regulators and noted that Commerzbank was, at that time, overwriting USD transactions requested by Iranian entities to avoid detection by United States and New York officials.
- i) In June of 2004, Commerzbank employees and Iranian-owned Bank Melli devised another system to circumvent United States and New York regulators. The scheme? Use checks.

- j) The Commerzbank rationale was “[t]he checks do [not] feature stamps or similar, but rather just signature and display no evidence of an Iranian background and thus can be cleared without any problem.”
- k) On July 1, 2004, Commerzbank provided Bank Melli with 500 checks for a USD account that only utilized only the Bank Melli account number, not its name. In only two months, Bank Melli was able to clear 108 checks totaling over two million USD.

1704. Commerzbank New York employees, despite being in a superior position to determine what types of payments would be appropriate under United States and New York law, were intentionally kept in the dark by Commerzbank management in an effort to maintain the Iranian USD conversion business. As a result, the illegal transactions continued unabated.

1705. In addition to laundering funds for Iranian banks, Commerzbank also intentionally laundered USD transactions for the sanctioned Iran Proxy IRISL.<sup>175</sup>

1706. In January of 2005, Commerzbank New York rejected USD payments to Lancelin Shipping Company, Ltd., a special purpose entity owned by IRISL.

1707. Based on this rejection, Commerzbank took it upon itself to develop a “safe payment” solution to the problem of IRISL having its USD transactions through Lancelin blocked by United States regulators.

1708. The “safe payment” solution was, in essence, a corporate shell game noting that “payments which are sent through . . . a subsidiary are unlikely to be rejected to our present knowledge.”

1709. Ultimately, in 2006, the OFAC filter was updated at Commerzbank New York with a more robust filter for special purpose entities. As such, USD transactions for companies used for the IRISL “safe payment” method began to get blocked. As more payments were

---

<sup>175</sup> See Section VII(F)(5) for further discussion regarding IRISL.

rejected, Commerzbank employees altered the “safe payment” strategy to shift the sanctioned payments through other IRISL special purpose entities that would not be picked up by the OFAC filter.

1710. Establishing the callous level of intent and motive for this purposeful evasion of United States New York law, Commerzbank began charging IRISL four times which it would charge a normal customer for a non-sanctioned USD transaction.

1711. Commerzbank justified the increase in cost “by providing no details which are currently subject to the OFAC embargo database, the risk of payments being frozen or rejected by US banks or their subsidiaries will be significantly reduced.”

1712. When a new head of Global Compliance was installed at Commerzbank, the employee solicited input from subordinates of issues that needed attention. A response from a Commerzbank New York employee states “persistent disregarding of OFAC rules by foreign businesses. Hamburg is notorious for it.”

1713. Illustrative of the volume of activity taken in derogation of United States and New York law on behalf of IRISL, just between September 10, 2008 and December 31, 2008, after IRISL had been placed on the OFAC sanctions list, Commerzbank processed \$40 million dollars in USD transactions for IRISL through Commerzbank New York and other United States financial institutions.

1714. Commerzbank also engaged in processing illegal USD transactions on behalf of Iranian entities through a correspondent bank in the United States, so Commerzbank New York “would not be involved” in the event “the going got tough.” Commerzbank used the following United States financial institutions to clear and settle some of its illegal transactions:

- a) HSBC Bank USA;

- b) Standard Chartered Bank, NY; and
- c) Deutsche Bank & Trust Co. Americas.

1715. According to the CHIPS-NY website, Commerzbank AG used, *inter alia*, the following U.S. financial institutions in New York to clear and settle its Eurodollar transactions:

- a) Commerzbank New York (identified by CHIPS-NY participant number 0804 and Fedwire number 026008044);
- b) Defendants HSBC Bank USA, N.A. (identified by CHIPS-NY participant number 0108 and Fedwire number 021001088);
- c) Defendants SCB's New York branch (identified by CHIPS-NY participant number 0256 and Fedwire number 026002561); and
- d) Deutsche Bank Trust Co Americas (identified by CHIPS-NY participant number 0103 and Fedwire number 021001033).

1716. Once confronted by investigators from the United States DOJ, the New York District Attorney's office, and the United States Department of the Treasury, Commerzbank voluntarily performed a wide array of tasks in submission to the jurisdiction of those United States and New York entities, including the following:

- a) Records reviews, client interviews, making current and former employees available for interview to regulatory officials;
- b) paying for and allowing full access by an outside consultant to review evidence of the allegations, provide regular updates to the DOJ and the District Attorney's office, and providing a detailed written report of their findings, among other actions.

1717. Based on the prolific and illegal utilization of the United States financial system to launder money for Iranian entities uncovered by the United States and New York officials, Commerzbank agreed to a sweeping submission of jurisdiction to the United States District Court for the District of Columbia and the United States DOJ, including the following:

- a) Payment of a \$79 million dollar fine;

- b) Forfeiture of \$560,000,000 to the United States government;
- c) An agreement the amount paid as a sanction were funds involved in the illegal transactions and there is a substantial connection between the funds used to pay the sanctions and the illegal conduct involving Iran;
- d) An agreement to fully cooperate in any future investigation relating to the laundering of money for Iranian entities, including an agreement to make employees available for interview and the provision of testimony;
- e) Provide information sufficient to allow the authentication of any document necessary for purposes of admission of documents or testimony into evidence in proceedings in the United States;
- f) An ongoing obligation to inform the DOJ of any additional illegal conduct that comes to light through its own internal investigation;
- g) An extensive revision of the Commerzbank corporate compliance program designed to detect and prevent violations of OFAC regulations, including:
  - i. Strict application of the OFAC sanctions list to all USD transactions;
  - ii. Not knowingly undertake any USD transactions prohibited by United States law, including those with Iran and Iranian entities;
  - iii. Continue to complete Financial Economic Crime sanction training for its employees who deal in USD transactions;
  - iv. Require the use of proper SWIFT message format for USD transactions rather than other, less transparent formats;
  - v. Abide by all elements of the cease and desist order issued by the Federal Reserve System;
  - vi. Abide by all elements of the settlement agreement reached with the DFS;
  - vii. Implement and pay for an outside compliance consultant;
  - viii. Report to the Department of Justice every 90 days regarding implementation of the compliance measures agreed to;
  - ix. At the completion of the terms of the agreement, the Chief Executive Officer of Commerzbank must certify that compliance has been achieved;
  - x. Notify the Department of Justice of any additional investigations commenced by any other entity;

- xi. If Commerzbank does not comply with the terms of the agreement, that it will be subject to criminal prosecution for its actions, including foregoing any statute of limitation defense and other evidentiary defenses it may have;
- xii. Ensure that any sale of Commerzbank or assets of the company shall include the compliance obligations expressed in the agreement transfer with the sale; and
- xiii. Not make any public statement or comment inconsistent with the acceptance of responsibility for illegally laundering money on behalf of Iran and other sanctioned entities.

1718. Because of the prolific nature of its use of the United States financial system to launder money for Iran and Iranian entities, Commerzbank also entered into a separate Consent Order with the DFS, which obligated Commerzbank to submit to the jurisdiction of the State of New York in the following ways:

- a) Payment of a civil monetary penalty of \$610,000,000;
- b) Implement an independent monitor, selected by the State of New York, for the term of approximately two years, to conduct a review of compliance programs within Commerzbank, including its compliance with OFAC regulations, whose responsibility it would be to:
  - i. Report on the extent to which the Commerzbank corporate governance contributed to the widespread illegal money laundering;
  - ii. Analyze and report on the thoroughness of Commerzbank's existing OFAC compliance program;
  - iii. Analyze and report on the organizational structure and competence of Commerzbank's then existing OFAC compliance and the competence of this structure;
  - iv. Analyze and report on the reasonableness and adequacy of any remedial plan implemented by Commerzbank with respect to OFAC compliance;
- c) Full compliance and cooperation with the independent monitor, including access to all necessary documents and personnel;

- d) Provide the State of New York with an action plan based off the recommendations of the independent monitor for compliance with OFAC regulations;
- e) Submit to the independent monitor by allowing it to oversee the implantation of the corrective measures proffered by Commerzbank; and
- f) Terminate four employees who were directly involved in the improper conduct, in addition to the firing of the compliance officer for Commerzbank New York.

1719. In terms of its Settlement Agreement with OFAC, based on the conduct set forth above, Commerzbank agreed:

- a) That it had terminated, among other things, all of the illegal conduct described herein with respect to Iran and other sanctioned entities;
- b) That it would maintain policies and procedure resulting from the agreements with the Department of Justice and the State of New York that would minimize, and prohibit if possible, the risk of similar conduct in the future; and
- c) To provide the Department of the Treasury copies of all reports submitted to the United States Federal Reserve relating to its illegal conduct described herein.

##### **5. Barclays' Participation in the Conspiracy**

1720. Barclays agreed to, and participated in, the Conspiracy.

1721. Beginning by at least the mid-1990s and continuing through at least 2006, Barclays had a continuous, ongoing relationship with Iran and its Agents and Proxies.

1722. During that time, Barclays transferred at least \$500,000,000 on behalf of designated persons in violation of U.S. sanctions, including Iranian entities.

1723. Further, Defendant Barclays knew that such transfers were funding the terrorists responsible for the Terrorist Attacks.

1724. Until at least May 2008, Defendants Barclays maintained correspondent banking relationships with several Iranian Bank co-conspirators, including Bank Saderat and Bank Melli.

1725. Barclays is a member of SWIFT-Brussels and has historically used the SWIFT-NET system to transmit and receive international payment messages to and from financial institutions around the world.

1726. Barclays originally processed USD payment messages through numerous global locations.

1727. Over time, Barclays consolidated its USD payment processing so the payments were predominately processed at Barclays' Payment Processing Centre located in Poole, England ("Poole").

1728. Barclays knowingly and willfully engaged in conduct that caused its New York branch and other financial institutions in the United States to process Eurodollar payment transactions in violation of U.S. sanctions.

1729. As part of this effort to evade U.S. sanctions against Iran, Barclays:

- a) Provided Iran and its Agents and Proxies with expert advice and then followed instructions from Iran and its Agents and Proxies (instructions that Iran and its Agents and Proxies would not have known to provide but for the expert advice Barclays and all other Defendants provided to them) not to mention their names in USD payment transaction messages sent to Barclays-New York and to other U.S. financial institutions for clearance and settlement in USD funds;
- b) Routed transactions through an internal Barclays sundry account, thereby hiding the payment transactions' connection to Iranian entities;
- c) Amended or reformatted SWIFT-NET payment order messages to remove information identifying Iranian entities involved in the transfer of USD funds; and
- d) Re-sent Iranian entities' SWIFT-NET MT 103 payment order messages as cover payments to take advantage of the lack of transparency as to the ultimate originator/beneficiary that was achieved by using the MT 202 bank-to-bank cover payment message format.

1730. Beginning in 1987, and following the expert advice provided by Defendants, Bank Melli Iran instructed Barclays to process USD transactions in favor of Bank Melli's

London branch by referencing only Bank Melli's Eurodollar account number at Midland Bank Plc and without referencing Bank Melli's name.

1731. Based on the expert advice provided to it by Defendants, Bank Melli further instructed Barclays to send separate payment order instructions, which included full details about the Eurodollar payment transactions to Midland Bank Plc and Bank Melli's London Branch.

1732. In response, Barclays memorialized Bank Melli's instructions for Eurodollar market transactions in a memorandum sent by its Head Office to Barclays' international offices, and, as early as the late 1990s, included them in Barclays' "List of Correspondents," which contained information related to Barclays' correspondent banking relationships and assisted Barclays' employees in illegally effectuating international payment transactions involving USD funds with Iran and its Agents and Proxies.

1733. Barclays' List of Correspondents contained instructions on how to process payments for both sanctioned and non-sanctioned banks with which Barclays had correspondent relationships.

1734. Over time, the List of Correspondents grew to include instructions for payments related to several of Barclays' correspondent bank clients and included instructions to use cover payments (SWIFT-NET MT 202 payment order messages) when processing payments in USD funds for clearing and settlement in the United States, and omitting the names of U.S.-sanctions targets from the payment order messages so that U.S. financial institutions could not identify the sanctions nexus of the payments.

1735. In a November 1987 Head Office Circular, Barclays distributed payment instructions received from an Iranian bank directing Barclays "to amend the procedures

governing the transfer of U.S. Dollars for any purpose in favour of our London branch” and to route such payments “without mentioning the name of our bank.”

1736. The reason for, and effect of, these instructions was to disguise Iranian sanctioned entity payments from Barclays’ correspondents in the United States so that such correspondents would unwittingly process the illegal payments.

1737. Barclays’ employees followed the instructions in the List of Correspondents when processing USD payments involving sanctioned Iranian banks, thereby ensuring the name of the bank would not appear in any MT 202 cover payment messages sent to Barclays’ New York branch for clearing and settlement through CHIPS-NY and FRBNY. For example, with regard to USD payments sent on behalf of an Iranian bank, the List of Correspondents stated, “[t]he cover MT202 for the direct Payment Order to be arranged by the remitting Bank without mentioning [the Iranian bank’s] name ....” (underlined in the original).

1738. Barclays’ List of Correspondents also contained instructions to contact the remitter or beneficiary for routing instructions for certain payments of USD funds involving Iranian sanctioned entities.

1739. The general instructions for Iranian banks stated:

#### USD PAYMENTS TO IRAN

Certain payments may be blocked by the US Authorities. Therefore, any branch with a USD transfer is advised to contact the remitter beneficiary or beneficiary’s bankers to request specific routing instructions.

1740. Barclays’ standard operating procedures allowed and even educated its employees on how to bypass the sanction screening algorithms in both Poole’s and the U.S. financial institution’s OFAC filters to permit illegal payment transactions in USD funds.

1741. Pursuant to these “standard” procedures, when the Poole filter identified a Eurodollar payment transaction that referenced an Iranian entity, that payment order message was stopped for further review by Barclays’ employees in Poole.

1742. If the Poole-based employees found the payment order message referenced an Iranian entity, they would follow one of the following procedures: (i) return the payment order message to the remitting entity via a pre-formatted fax cover sheet; (ii) alter or delete fields in the SWIFT-NET payment order message; or (iii) change the message type from a serial payment (MT 103) to a cover payment (MT 202) in order to hide any connection to the Iranian entity.

1743. The then-Senior Manager for Barclays Group Payments Industry Management in Poole explained that if the MT 202 payment order message contained beneficiary information that caused it to be stopped by the OFAC filter in the U.K., that information was removed to ensure the payment transaction was not stopped by the OFAC filter when resubmitted.

1744. The same Senior Manager noted that he was aware that Defendants Barclays’ payment operators amended payment order messages in order to facilitate the transfer of USD funds to Iran and that this was a “common practice” at Barclays.

1745. As noted above, consistent with Barclays’ “standard” procedures, when an Iranian payment was flagged by the Poole OFAC filter, Barclays’ employees generally returned the flagged payment order message to the original remitting bank.

1746. Barclays’ employees used a specific fax cover sheet to advise the remitting area of Barclays that the payment message had been cancelled and would further identify the specific words in the payment message that had caused the message to be stopped by the Poole sanctions screening filter.

1747. The Barclays fax cover sheet contained the following language:

OFAC ITEM: Wording below is contained in the message and does not comply with the [OFAC] regulations applicable to all payments sent via the U.S.A. Payments to U.S.A. must NOT contain the word listed below.

1748. Subsequently, because Barclays was advising the remitting bank of the prohibited language, some of these payment order messages would thereafter be re-sent by the remitting bank on the SWIFT-NET network without the “offending” language.

1749. This deliberate omission enabled the payment order message to pass through the Poole sanctions screening filter without being blocked, and then clear and settle in USD funds by Barclays’ New York branch and unwitting U.S. financial institutions.

1750. In November 2001, the use of the fax cover sheet was identified by Barclays’ internal auditors as problematic because (according to a Barclays internal audit report) “without adequate guidance the recipient of the fax advice may not be aware of the implications and may merely remove the offending text and re-submit the payment without any wider consideration.”

1751. In early 2002, as a result of this internal audit report, the language of the fax template was re-worded in an attempt to mitigate these issues. The fax language was changed to:

OFAC ITEM: Wording below is contained in the message and does not comply with the U.S.A. / U.K. / E.C. / U.N. Sanctions.

1752. Despite the altered wording in the fax cover sheet, no implementing guidance was circulated, and Barclays’ “standard” practices nevertheless continued, as did the resubmission of prohibited OFAC-sanctioned transactions with the offending text removed.

1753. Barclays’ employees generated internal correspondence that documented Barclays’ awareness and acceptance of the fact transactions were being processed via MT 202 cover payments for the specific purpose of hiding the identity of Iranian entities in order to ensure that Barclays could continue its unfettered processing of USD funds transfers involving Iranian entities through Barclays’ New York branch.

1754. For example, one Barclays employee explained in an email:

[W]e can get around [OFAC seizure] by sending only cover payments to US banks and then make MT103 direct to beneficiary's bank. The MT202 cover must not mention of [sic] the offending entity which could cause funds to be seized. A good example is Cuba which the US says we shouldn't do business with but we do.

1755. Barclays' employees understood the advantage of using bank-to-bank cover payments. The cover payment message format (MT 202), with its limited information fields, was a better mechanism to process OFAC-prohibited transactions than using a more detailed serial payment message format (MT 103).

1756. A Barclays employee noted in an email: "If we were to route the payment via the serial payment method ... the payment would clearly be seized by the US authorities" but by using cover payments, "the US Treasury [would] remain blissfully unaware of [the payment's] existence."

1757. In December 2002, internal correspondence also brazenly acknowledged Barclays' use of MT 202 cover payment messages to detour U.S. Iranian sanctions, stating:

To circumvent US legislation, [Barclays is] currently rout[ing] US\$ items for sanctioned institutions via unnamed account numbers, without mention of the sanctioned party. For customer transfers, payment cover is routed via MT202 to New York, naming only the account holding bank. A direct MT103 is then [sic] sent to the account holding bank. Further investigation suggests that we are carrying out this practice on behalf of four [Iranian bank] customers....

1758. A January 2004 report provided to Barclays' Group Risk Oversight Committee noted that a recent failure "illustrat[ed] why the whole sanctions process needs to be reviewed and brought up to date."

1759. In July 2004, an internal assessment of Barclays' payments processing explained: Cover payments are an issue for this project as they are effectively a way of by passing [sic]

sanctions.... There is nothing in these payment messages [MT 103 and MT 202] that identifies them as linked for the purpose of screening.

1760. In April 2005, Barclays noted in an internal memo the risk of using MT 202 cover payments rather than MT 103 serial payments, and also acknowledged that other financial institutions such as Defendants facilitated payments for Iran in the same manner:

Changing to different message types would be much more expensive to us. Moral risk exists if we carry on using cover payments but that is what the industry does. I[n] M[y] H[umble] O[pinion] we should carry on using cover payments and accept that there is a risk of these being used on occasion to hide true beneficiaries (who may or may not be sanctioned individuals or entities).

1761. In the spring of 2006, Barclays' senior management learned that four cover payments involving sanctioned parties had been routed through Barclays' New York branch and were processed because the cover payments did not mention the sanctioned beneficiary or originator.

1762. Barclays also continued to facilitate unlawful payments on behalf of Bank Saderat after Barclays knew that Bank Saderat had been designated an SDGT for enabling the transfer of USD funds to Hezbollah.

1763. Barclays also continued facilitating unlawful Eurodollar payments on behalf of Bank Melli after Barclays knew that Bank Melli had been designated by the United States in part for its enabling the transfer of USD funds to the IRGC.

1764. On August 18, 2010, the Department of Justice announced that Barclays had entered into a DPA with federal and New York State prosecutors, and agreed to forfeit \$298 million dollars in connection with violations of IEEPA and the Trading with the Enemy Act.<sup>176</sup>

---

<sup>176</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPAs entered into between Barclays and the New York Department of Financial Services and the DOJ on or about August 16, 2010, as if fully set forth herein.

1765. A criminal information was filed on August 16, 2010, in the U.S. District Court for the District of Columbia charging Barclays with one count of violating the IEEPA, and one count of violating the Trading with the Enemy Act. Barclays waived indictment, agreed to the filing of the information, and accepted and acknowledged responsibility for its criminal conduct.

1766. In the press release announcing the DPA, then-FBI Assistant Director-in-Charge Janice K. Fedarcyk was quoted stating:

Barclays Bank has admitted a decade-long pattern of violating U.S. banking laws, and taking certain steps to conceal prohibited transactions. Corporate responsibility entails more than just acting discreetly on behalf of one's clients. It means, first and foremost, acting lawfully.

1767. From as early as the mid-1990s until September 2006, Barclays knowingly and willfully moved or permitted to be moved hundreds of millions of dollars through the U.S. financial system on behalf of banks from Cuba, Iran, Libya, Sudan and Burma, and persons listed as parties or jurisdictions sanctioned by OFAC in violation of U.S. economic sanctions.

1768. Based on this illegal conduct, in 2010, Barclays also entered into a Settlement Agreement with OFAC, related to its illegal laundering of funds from countries which the United States had determined to be enemy states, and state sponsors of terrorism, such as Iran.<sup>177</sup>

1769. The conduct engaged in by Barclays with respect to performing illegal USD transactions for Iran and Iranian entities, to which Barclays has expressly admitted through the DPA and Settlement Agreement, is expansive.

1770. From the mid-1980s through at least 2008, Barclays violated both New York and United States law by knowingly and intentionally moving, or permitting to be moved, hundreds

---

<sup>177</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Settlement Agreements entered into between Barclays and the United States Department of Treasury in August 2010, as if fully set forth herein.

of millions of dollars through the United States financial system on behalf of entities and banks from countries sanctioned by OFAC, including Iran.

1771. Barclays' criminal conduct consisted of, among other things following the instructions of Iran and Iranian entities to not mention their names in USD payment message sent to Barclays New York, and other financial institutions throughout the United States, to prevent such payment transactions from being seized or investigated.

1772. As another example, as early as 1987, Bank Melli Iran instructed Barclays to process its USD transactions in favor of Bank Melli's London branch by referencing only Bank Melli's account number at Midland Bank, Plc, without making any reference to Bank Melli. This became the standard internal procedure at Barclays for Bank Melli.

1773. As another method of circumventing United States law, Barclays would route USD payments for Iran through internal Barclays sundry accounts to hide the fact the payments were for Iranian entities. The Department of Justice and the District Attorney's Office of New York found, and Barclays agreed, the net effect of Barclays using internal sundry accounts was that Barclays New York would believe that a payment was originating from Barclays when in reality it was from a sanctioned entity, such as an Iran sanctioned entity, thereby ensuring the transaction would evade detection and be processed by Barclays New York or other correspondent United States financial institutions.

1774. In the event an impermissible USD transaction request was received by Barclays that was not adequately sanitized to avoid detection, Barclays would reformat such USD payment messages to remove information identifying Iranian entities in the payment request. This practice was widespread and intentional.

1775. For example, Barclays New York maintained an OFAC filter that would screen incoming payment requests against a list of sanctioned entities. Items flagged by OFAC filter would then be held, investigated, rejected or blocked pursuant to United States and New York law. The Barclays office in Poole, England also had an OFAC filter program. However, the express purpose of the OFAC filter in Poole was to be an interdiction filter – designed to prevent suspect funds from being seized in the United States by the Barclays New York OFAC filter. Once suspect transactions were identified in Poole, the Barclays employees would ensure the transactions were sterilized to prevent detection by United States and New York regulators.

1776. Barclays would, in some instances, return the request to the remitting bank and simply inform them the inclusion of specific words or entities would draw an OFAC filter flag and to please redo the payment request without the offending words.

1777. Once sanitized, these requests would then be sent to Barclays New York and other United States financial institutions, for processing.

1778. These procedures and processes designed to flout United States and New York law were well known throughout Barclays. An email from the Compliance Director in 2001 to the then Head of Group Compliance that “[f]or Iran and Libya the published internal procedures include directions to make transfers in US dollars which circumvent the constraints and breach OFAC sanctions.”

1779. In addition to overtly manipulating USD transactions in the payment stream, Barclays acted to prevent its employees from being educated about United States sanction law.

1780. Barclays admitted to not training its non-United States employees on Barclays’ obligations under United States’ sanction law, and did not provide any meaningful information to

its employees about OFAC regulations, thereby increasing the chances that illegal transactions would be processed through United States financial institutions.

1781. Barclays efforts on behalf of Iranian entities caused these manipulated transaction requests, that should have otherwise been held, investigated, rejected or blocked pursuant to United States and New York law, to be paid.

1782. This conduct also caused Barclays' operations in the United States, particularly the New York branch, to (1) not be able to file necessary and appropriate paperwork pursuant to the Bank Secrecy Act and other paperwork required by OFAC and the DFS designed to root out such illegal payments; (2) cause false information to be recorded in the official records of United States financial institutions; and (3) not make banking records that are otherwise required by United States and New York law.

1783. According to the Department of Justice and the District Attorney of New York, the net effect of these intentional efforts by Barclays targeting the United States financial system caused approximately \$500 million dollars in prohibited transactions to be processed through the United States, a significant portion of that was steered back to Iran for the purposes discussed in this Complaint.

1784. As a result of the foregoing conduct, and other similar conduct designed to convert foreign currency into USD for sanctioned Iranian entities, Barclays was charged in a two-count criminal information in the United States District Court for the District of Columbia in August of 2010 alleging Barclays violated 50 U.S.C. app. §§ 5, 16 (Trading with the Enemies Act), and the IEEPA, 50 U.S.C. § 1705.

1785. Barclays was required to submit to the jurisdiction of United States courts, work in conjunction with the DOJ, United States Department of the Treasury, and the District

Attorney's office for New York over the course of the next two years to ensure compliance with a host of matters required by a DPA entered into by Barclays and federal and New York officials on August 16, 2010. In the DPA, Barclays agreed:

- a) That it acknowledged and accepted responsibility for the conduct described above;
- b) That funds it held were forfeitable pursuant to the charges alleged;
- c) That in lieu of a forfeiture proceeding, it would pay the United States \$149,000,000 USD based on its illegal conduct;
- d) Agree to a continuing relationship with the DOJ and the District Attorney of New York in which it would do a number of things in an attempt to ensure its company no longer tried to circumvent United States law for the purpose of laundering money on behalf of sanctioned Iranian entities, or face prosecution in the United States, including:
  - i. Conducting in-depth training of Barclays employees on United States sanctions involved in the processing of USD payments and securities, and certify to the United States that such training had been completed;
  - ii. Develop written policies to require that SWIFT policies and protocols are being followed and certify to the United States that such training has been completed;
  - iii. Maintain all documents associated with this investigation by the United States for a period of five years;
  - iv. Completely and fully disclose to the United States all documents having anything to do with the allegations of payments to sanctioned entities, including Iranian entities;
  - v. Provide witnesses and testimony to the United States in any criminal or civil proceeding relating to its payments made to sanctioned entities, including Iran;
  - vi. Implement procedures to ensure that all compliance officers in charge of sanctions are made aware of any known request or attempt by any sanctioned entity that could be considered an attempt to circumvent or evade United States sanction law. These reports must be provided to Barclays' Head of Compliance and Regulatory Affairs who in turn shall report this information to the United States and the State of New York;

vii. Comply with all remedial measures implemented by the United States Federal Reserve System and the Office of Foreign Asset Control of the Department of the Treasury as a result of its evasion of sanctions described herein on behalf of sanctioned Iranian entities.

- e) To waive jurisdiction and venue in the United States District Court for the District of Columbia;
- f) To be prosecuted for the crimes charged if it were to materially breach the substance of the agreement reached with the United States;
- g) To not make any public statement contradicting, excusing or justifying its conduct in laundering money for sanctioned Iranian entities, among others; and
- h) To include in any sales agreements for any of its operations involved in the transmission of USD a requirement the purchasing entity be bound by the terms and conditions of the DPA.

1786. In its Settlement Agreement with the United States Department of the Treasury, Barclays agreed to forfeit \$176,000,000 to OFAC and remains subject to its jurisdiction pending completion of the obligations owed to the DOJ and the State of New York.

## **6. BNP's Participation in the Conspiracy**

1787. BNP agreed to, and participated in, the Conspiracy.

1788. From at least 1997 through November, 2012, BNP knowingly and intentionally structured, conducted, and concealed USD transactions from regulators on behalf of sanctioned entities, including Iranian entities. These intentionally opaque USD transactions were processed through BNP's office in New York and other financial institutions throughout the United States. The illegal BNP transactions include a variety of trade finance instruments on behalf of or that involved parties subject to U.S. sanctions on Iran and routed the USD payments to go through the United States pursuant to those instruments; correspondent banking or retail banking transactions to or through the United States that involved the interest of a person subject to U.S. sanctions on Iran; processing a number of payments to or through the United States related to syndicated loans involving Iranian parties. Federal government authorities, as part of the

investigation into BNP, probed approximately \$100 billion of transactions. They found that that \$30 billion of that amount were concealed, as part of BNP's effort to avoid U.S. sanctions. New York's Department of Financial Services identified \$190 billion in transactions that broke federal and state laws, including false books and records violations.

1789. Beginning at least as early as 2002, BNP entered into an agreement with Iran to provide it with access to billions of USD in violation of U.S. and international sanctions on Iran. BNP provided Iran with at least \$160 billion USD through 2012 and ultimately plead guilty to violating U.S. and New York law in 2014. As part of the guilty plea to the criminal charges, which included conspiring with Iranian and Sudanese sanctioned entities to violate U.S. sanctions, BNP agreed to pay an \$8.9 billion fine to federal and state authorities, terminate senior executives, and suspend U.S. dollar clearing operations for one year at business lines in which the misconduct centered, starting in 2015. BNP was also sentenced to five years probation.

1790. BNP received these punishments because its violations of sanctions supported global terrorism. "The most important values in the international community—respect for human rights, peaceful coexistence, and a world free of terror—significantly depend upon the effectiveness of international sanctions," said District Attorney Vance in the DOJ press release accompanying the announcement of BNP's guilty plea. As found by the Superintendent of Financial Services for New York State, Benjamin Lawsky, BNP "illegally funneled money to countries involved in terrorism and genocide" and that "multiple senior executives" knew that BNP was involved in that long-standing scheme. New York Governor Andrew Cuomo likewise stated in connection with the proceedings against BNP: "New York State will not allow companies to break the law, especially when they put our national security at risk . . . . This enforcement action should serve as a warning to any company that provides financial support to

global terrorism and enables human rights atrocities. . . .” Assistant U.S. Attorney Andrew Goldstein, representing the United States at BNP’s criminal sentencing stated “without BP acting effectively as its US central banker, [Sudan and Sudanese SDNs] would not have had access to the US dollar markets.”<sup>178</sup>

1791. Numerous other officials in the U.S. government similarly concluded that BNP willfully violated U.S. sanctions, provided rogue nations that support terrorism with access to the U.S. financial system, and did not cooperate with law enforcement when it was finally caught, as reflected in the DOJ press release:

- a) “BNP Paribas went to elaborate lengths to conceal prohibited transactions, cover its tracks, and deceive U.S. authorities. These actions represent a serious breach of U.S. law,” Attorney General Holder said. “Sanctions are a key tool in protecting U.S. national security interests, but they only work if they are strictly enforced. If sanctions are to have teeth, violations must be punished. . . .”
- b) “BNP ignored US sanctions laws and concealed its tracks. And when contacted by law enforcement it chose not to fully cooperate,” Deputy Attorney General Cole said. “This failure to cooperate had a real effect—it significantly impacted the government’s ability to bring charges against responsible individuals, sanctioned entities and satellite banks. This failure together with BNP’s prolonged misconduct mandated the criminal plea and the nearly \$9 billion penalty that we are announcing today.”
- c) “By providing dollar clearing services to individuals and entities associated with Sudan, Iran, and Cuba – in clear violation of U.S. law – BNPP helped them gain illegal access to the U.S. financial system,” said Assistant Attorney General Caldwell. “In doing so, BNPP deliberately disregarded U.S. law of which it was well aware, and placed its financial network at the services of rogue nations, all to improve its bottom line. Remarkably, BNPP continued to engage in this criminal conduct even after being told by its own lawyers that what it was doing was illegal.”
- d) “BNPP banked on never being held to account for its criminal support of countries and entities engaged in acts of terrorism and other atrocities,” said U.S. Attorney Bharara. “But that is exactly what we do today. BNPP, the world’s fourth largest bank, has agreed to plead guilty and pay penalties of almost \$9

---

<sup>178</sup> Transcript of Guilty Plea Hearing, United States v. BNP Paribas, No. 14-CR-00460 (LGS) (July 9, 2014), at 31-32

billion for performing the hat trick of sanctions violations, unlawfully opening the doors of the U.S. financial markets to three sanctioned countries, Sudan, Iran, and Cuba. For years, BNPP provided access to billions of dollars to these sanctioned countries, as well as to individuals and groups specifically identified and designated by the U.S. government as being subject to sanctions. The bank did so deliberately and secretly, in ways designed to evade detection by the U.S. authorities. . . .”

1792. The District Court at BNP’s sentencing expressed similar views regarding BNP’s conduct when it addressed some of the victims of state-sponsored terrorism that were present at the sentencing: “Your presence in the room emphatically reminds BNPP and other banks contemplating similar conduct of the pain and suffering states they illicitly transacted with can inflict, and your being here also illustrates why the United States imposes sanctions on the states in the first place.”

1793. For over a decade, BNP provided USD clearing services on behalf of Sudanese, Iranian, and Cuban parties with a value of more than \$190 billion which were settled through its New York Branch and other New York-based financial institutions. Several BNP branches, including Paris, London, Geneva, Rome and Milan, developed and implemented policies and procedures to systematically conceal at least \$160 billion in U.S. dollar-denominated payments on behalf of Iranian customers. At least \$650 million in transactions from 2004 to 2012 involved sanctioned Iranian entities, including transactions for a petroleum company based in Dubai that was effectively a front for an Iranian petroleum company and an Iranian oil company. BNP continued these illegal transactions for nearly two years after the bank had commenced an internal investigation into its sanctions compliance and pledged to cooperate with the government.

1794. AS part of BNP’s guilty plea, it admitted, *inter alia*, the following:

- a) From 2002 up through and including 2007, BNPP, predominantly through its Swiss-based subsidiary, BNPP Geneva, conspired with numerous Sudanese banks

and entities as well as financial institutions outside of Sudan to violate the US. embargo by providing Sudanese banks and entities access to the US. financial system... despite the Government of Sudan's role in supporting international terrorism and committing human rights abuses during this time period.

- b) In 1997, shortly after the imposition of U.S. sanctions against Sudan, BNPP Geneva agreed to become the sole correspondent bank in Europe for Sudanese Government Bank 1 [Central Bank of Sudan], which, as noted above, was designated by OFAC as an SDN. Sudanese Government Bank 1 then directed all major commercial banks located in Sudan to use BNPP Geneva as their primary correspondent bank in Europe. As a result, all or nearly all major Sudanese banks had U.S. dollar accounts with BNPP Geneva.
- c) BNPP's central role in providing Sudanese financial institutions access to the U.S. financial system, despite the Government of Sudan's role in supporting terrorism and committing human rights abuses, was recognized by BNPP employees. For example, in...March 2007, another senior BNPP Paris compliance officer reminded other high-level BNPP compliance and legal employees that certain Sudanese banks with which BNPP dealt "plays a pivotal part in the support of the Sudanese government which ... has hosted Osama Bin Laden..."
- d) BNPP continued to process transactions involving Sudanese Sanctioned Entities--despite being well aware that its conduct violated U.S. law -because the business was profitable and because BNPP Geneva did not want to risk its longstanding relationships with Sudanese clients. For example, in a July 2006 Credit Committee Meeting of BNPP's general management, despite expressing a concern about BNPP's role in processing U.S. dollar transactions with Sudanese Sanctioned Entities, BNPP's senior compliance personnel signed off on the continuation of the transactions. An email summarizing that meeting explained that "[t]he relationship with this body of counterparties is a historical one and the commercial stakes are significant. For these reasons, Compliance does not want to stand in the way of maintaining this activity for ECEP and [BNPP Geneva].
- e) In February 2007,'a senior BNPP Paris compliance officer specifically recognized the significance of the Sudanese business for BNPP Geneva: For many years, the Sudan has traditionally generated a major source of business for BNPP Geneva including transactions such as investment held on deposit. The existence of a dedicated desk for this region, GC8, for which the Sudan is one of the largest customers, relationships developed with directors of Sudanese financial institutions and traditional practices have over the years led to a major source of income, which is now recurring income.

1795. BNP provided correspondence services to Sudanese bank al Shamal Islamic Bank through its subsidiary United European Bank, even though BNP senior management knew, or

was deliberately indifferent to the fact that the al Shamal was owned (in part) by Usama bin Laden and funded al Qaeda operations.

1796. In September 2001, after the 9-11 attacks, Senator Carl Levin testified before the Senate Committee on Banking, Housing and Urban Affairs that evidence suggests that Bin Laden “remains the leading shareholder” of Al Shamal and that he may still use the bank’s facilities.

1797. BNP knew, or was deliberately indifferent to the fact that SDGT Adel bin Abdul-Jalil Batterjee (UBL’s brother-in-law) served as Chairman of al Shamal Islamic Bank and was one of its principal shareholders during the time BNP was illegally providing USDs to al Shamal Islamic Bank. In 2004, the United States designated Batterjee as a terrorist financier and a UN Security Council placed him under a worldwide travel ban, financial embargo, and weapons embargo. In 2004, Stuart Levey, Undersecretary for the Treasury Department’s Office of Terrorism and Foreign Intelligence stated that:

Abdel Batterjee has ranked as one of the world’s foremost terrorist financiers, who employed his private wealth and a network of charitable fronts to bankroll the murderous agenda of al Qaida. A worldwide asset freeze, including in his home country of Saudi Arabia, will deal a serious blow to this key terrorist facilitator.<sup>179</sup>

1798. On August 14, 1996, the State Department issued a fact sheet on Bin Laden, which stated:

Usama bin... Laden is one of the most significant financial sponsors of Islamic extremism in the world today ...Bin Laden’s company, Al-Hirjrah for Construction and Development, Ltd...[and his] import-export firm, Wadi al-Aqiq Company Ltd. in conjunction with his Taba Investment Company, Ltd., secured a near monopoly over Sudan’s major agricultural exports in cooperation with prominent NIF members...Bin Laden and wealthy NIF members capitalized Al

---

<sup>179</sup> U.S. Treasury press release, “U.S. Treasury Designates Two Individuals with Ties to al-Qaida, UBL Former BIF Leader and al-Qaida Associate named under E.O. 13224.” (Dec. 21, 2004).

Shamal Islamic Bank in Khartoum. Bin Laden invested \$50 million in the bank...A joint Egyptian-Saudi investigation revealed in 1993 that Bin Laden business interests funnel money to Egyptian extremists, who used the cash to buy...weapons...Bin Laden remains a key financier behind the "Kumar" camp in Afghanistan, which provides terrorist training to al-Jihad and al-Gama'a al-Islamiyah members.

1799. Honorable John Bates found in connection with prior civil litigation against Sudan in connection with the 1998 East African Embassy Attacks:

Bin Laden and Al Qaeda also invested in Sudanese banks. This access to the formal banking system was useful for 'laundering money and facilitating other financial transactions that stabilized and ultimately enlarged bin Laden's presence in the Sudan.' For example, Bin Laden invested \$50 million in the Sudan's Al Shamal Islamic Bank, and these funds were used to finance Al Qaeda operations. Al Shamal Islamic Bank was known for financing terrorist operations, and bin Laden remained a leading investor of the bank long after he was expelled from the Sudan.<sup>180</sup>

1800. In 1998, Governor Mutasim Abdul-Rahim, Secretary General of the National Congress Party in Khartoum, as well as a spokesman for, co-founder of and major shareholder in Al Shamal issued a statement promoting jihad urging "all those who are able to carry a gun to join the [military training] camps...Jihad has now become an obligation that comes before any other duty." Mohamad Osman, "Sudanese students enroll for controversial military service." AP Worldwide (June 6, 1998).

1801. Mohammed S. Mohammed, General Manager of Al Shamal, acknowledged in a September 2001 press release that bin Laden held two accounts in the bank.

1802. Jamal Ahmed Al-Fadl ("Al-Fadl"), a former financial officer for bin Laden, testified that at least six Al Qaeda operatives held accounts in their own names at Al Shamal:

- Q. While you were in Sudan, did you handle money for Osama bin Laden?
- A. Could you repeat the question.
- Q. Did you work on the finances for Al Qaeda while you were in the Sudan?
- A. Yes.

---

<sup>180</sup> *Owens*, 826 F. Supp. 2d at 144) (emphasis added and internal citations omitted).

Q. Did you know where the bank accounts of Osama bin Laden and Al Qaeda were?

A. Yes.

Q. Do you know whose names they were in?

A. The bank account under Osama bin Laden in Bank Shaml [al Shamal Islamic Bank], Khartoum.

Q. That was under Osama bin Laden's true name?

A. Yes.

Q. Were there accounts in other names?

A. Yes.

1803. Wadi el-Hage ("El-Hage), former personal secretary for bin Laden convicted for his role in the bombings [of the U.S. embassies in 1998 by al Qaeda], also testified that bin Laden kept accounts at Al Shamal:

Q. When you worked for Osama bin Laden in the Sudan, how much were you paid?

A. \$1,200 a month.

Q. For how long did you work for him [Osama bin Laden]?

A. Almost two years.

Q. What Banks did you keep his money at?

A. Bank Al Shamar [Al Shamal].

1804. Al-Fadl<sup>181</sup> transported cash payments from Al Qaeda to Abu Ali, an affiliated jihadist organizations in Jordan, through funds maintained at Al Shamal:

Q. How did you carry the \$100,000?

A. In my bag with my clothes.

Q. Do you recall what kind of bills the \$100,000 was in?

A. I remember they all hundred bill.

Q. Sorry

A. They all hundred bill.

Q. They were all hundred dollar bills?

A. Yes.

Q. Who gave you the money?

A. Abu Fadhl, he bring it from Shamal Bank [Al Shamal] and he bring it to me.

---

<sup>181</sup> *United States v. Osama bin Laden*, No. S(7) 98 Cr. 1023 (S.D. N.Y.), Feb. 6, 2001 (transcript pp. 218–219, 233); Feb. 13, 2001 (transcript pp. 514–516); Feb. 20, 2001

1805. During the planning of these 1998 East African Embassy Attacks, Al-Fadl received \$250,000 from Al Shamal purchase a plane for Al Qaeda. The plane was used to coordinate Al Qaeda's efforts in preparation for the 1998 Embassy bombings, including flying bin Laden to a meeting in Teheran with the heads of the IRGC and Hizballah to plan the attacks on the embassies and arrange training for Al Qaeda operatives in Iran and Bekaa Valley, Lebanon.

1806. Moreover, from on or about July 15, 2005, to on or about November 27, 2012 alone, BNP processed at least 318 electronic funds transfers in the aggregate amount of \$1,182,075,543 to or through financial institutions located in the United States in apparent violation of the prohibitions against the exportation or re-exportation of services from the United States to Iran, 31 C.F.R. § 560.204. From at least 2009 and again from at least December 2011 to November 2012, BNP transferred at least \$686,600,000.00 on behalf of Iranian entities and persons in violation of U.S. sanctions.

1807. In processing transactions on behalf of these sanctioned entities, BNP engaged in a systematic practice, as directed from high levels of the bank's group management, of removing or omitting Sudanese, Iranian, or Cuban information from USD-denominated payment messages that it sent through the New York Branch and other non-affiliated New York-based U.S. financial institutions. This practice was done to "guarantee the confidentiality of the messages and to avoid their disclosure to any potential investigatory authorities." BNP's violations were particularly egregious in part because they continued for many years after other banks were sanctioned for similar violations; involved numerous schemes expressly designed to deceive regulators; and were committed with the knowledge of multiple senior executives.

1808. From at least 2004 up through and including 2012, BNP conspired with banks, including Defendants and Iran and/or its Agents and Proxies, as well as other entities located in

or controlled by countries subject to U.S. sanctions, other financial institutions located in countries not subject to U.S. sanctions, and others known and unknown, to knowingly, intentionally and willfully move at least \$8,833,600,000 through the U.S. financial system on behalf of sanctioned entities in violation of U.S. sanctions laws, including transactions totaling at least \$4.3 billion that involved SDNs.

1809. Among the means and methods by which BNP and its co-conspirators carried out the conspiracy were the following: BNP intentionally used a non-transparent method of payment messages, known as cover payments, to conceal the involvement of sanctioned entities in USD transactions processed through BNP Paribas New York and other financial institutions in the United States; BNP worked with other financial institutions to structure payments in highly complicated ways, with no legitimate business purpose, to conceal the involvement of sanctioned entities in order to prevent the illicit transactions from being blocked when transmitted through the United States; BNP instructed other co-conspirator financial institutions not to mention the names of sanctioned entities in USD payment messages sent to BNP Paribas New York and other financial institutions in the United States; BNP followed instructions from co-conspirator sanctioned entities not to mention their names in USD payment messages sent to BNP Paribas New York and other financial institutions in the United States; and BNP removed information identifying sanctioned entities from USD payment messages in order to conceal the involvement of sanctioned entities from BNP Paribas New York and other financial institutions in the United States. BNP provided expert advice, financial services, financial securities, and access to the U.S. financial system to make it all possible.

1810. For example, for one sanctioned Iranian client alone (referred to as “Iranian Controlled Company I”), from 2006 to 2012, BNP processed at least \$650 million in connection

with three letters of credit that facilitated the provision of liquefied petroleum gas to an entity in Iraq. The majority of those transactions—approximately \$586 million—occurred after OFAC revoked the U-turn Exemption, after the New York Country District Attorney’s Office and the DOJ approached BNP regarding its involvement with sanctioned entities, and after multiple other banks blocked BNP’s payments relating to Iranian Controlled Company I.

1811. BNP knew that Iranian Controlled Company 1 was controlled by an Iranian energy group based in Tehran, Iran (“Iranian Energy Group 1”). Its own internal Know Your Customer documentation on Iranian Controlled Company I showed that it was 100% owned by Iranian Energy Group 1. BNP’s documentation also showed that Iranian Energy Group I, and in turn Iranian Controlled Company 1, was 100% owned by an Iranian citizen.

1812. The transactions involving Iranian Controlled Company 1 began in approximately December 2006, at a time when the U-turn Exemption permitted certain transactions involving Iranian entities so long as those transactions were between two non-U.S., non-Iranian banks. BNP’s transactions involving Iranian Controlled Company 1 initially complied with the U-Tum Exemption. BNP issued its “Revised Group Policy on Iran” on September 24, 2007, and OFAC revoked the U-turn Exemption in November 2008. Despite this new bank policy and the revocation, BNP continued to process U.S. dollar transactions involving Iranian Controlled Company 1 through November 2012.

1813. On June 12, 2007, BNP Paribas Paris opened an account for a company incorporated in the UAE with an address listed in Dubai, UAE. An organizational chart submitted to BNP Paribas Paris indicated the company was part of a network of eight companies—four of which were incorporated in Iran—that comprised an Iranian energy group owned and controlled by an Iranian citizen ordinarily resident in Iran, who was also the sole

beneficial owner of the company maintaining an account at BNP Paribas Paris. According to BNP Paribas Paris's account opening materials (and a report the company produced to BNP Paribas Paris in 2007), many of the company's activities involved selling and transporting petroleum products to, from, or through Iran. The company's General Business Plan described its goals to increase a number of Iran-related activities over the following three years (2007-2010). Based upon the records made available to the government, the government concluded that BNP's outbound transactions through the United States on behalf of the company appeared to have violated the prohibition contained in § 560.204 of the Iranian Transactions and Sanctions Regulations because the benefit of these transactions was received in Iran.

1814. The company referenced above utilized its account at BNP Paribas Paris to receive payments related to its sale of Turkmen liquefied petroleum gas to Iraq. Between November 2008 and November 2012, BNP processed 114 transactions totaling approximately \$415 million on behalf of the company to or through the United States. Although the messages related to the transfers sent through the United States did include references to the company's name, they did not include references to Iran or to the company's Iranian ownership or connections. Most of the USD transfers BNP initiated on behalf of the company reached their intended beneficiary. On January 9, 2012, however, BNP Paribas Paris originated a \$500,000 wire transfer on behalf of the company, destined for a refinery in Turkmenistan, and an unaffiliated correspondent bank located in the United States stopped the transaction and requested additional details from BNP Paribas New York. BNP Paribas New York informed BNP Paribas Paris the unaffiliated correspondent bank was holding the payment "due to OFAC concern" and requested information about the payment, the company, the company's owners, and "anyway [sic] the transaction is related to Iran directly or indirectly." BNP Paribas Paris

contacted the company directly to relay the questions, and the response—which came from an email address belonging to the Iranian energy group noted above—denied any association between the company and Iran. A BNP Paribas Paris compliance officer reviewed and approved the response for transmission to the unaffiliated correspondent bank without verifying the information or consulting the customer profile form for the company. At the time of the transaction, the customer profile form included a handwritten note for the company that read “Iranian ownership.” In light of the available information, BNP appears to have had reason to know of the company’s connection to Iran, and it failed to pass any of that information on to the unaffiliated correspondent bank in response to its inquiry. Even after the rejected transaction described above, BNP failed to subsequently investigate either the payment or the company, despite the fact BNP Paribas Paris processed 64 additional transactions valued at over \$292 million on behalf of the company through the United States between January 2012 and November 2012, at which time BNP Group Compliance first learned about these transactions (BNP closed the company’s account on November 27, 2012).

1815. BNP also continued to process transactions on behalf of Iranian Controlled Company 1 even after other banks blocked payments that involved that company. In December 2011, a U.K. Bank (“U.K. Bank 1”) blocked a payment involving Iranian Controlled Company 1 and informed BNP that it would no longer do business with Iranian Controlled Company 1 because of its ties to Iran—thus putting BNP on notice, to the extent that it was not before, that transactions with Iranian Controlled Company 1 were impermissible. Moreover, in January 2012, a U.S. branch of a German bank (“German Bank 1”) rejected a payment made by BNP on Iranian Controlled Company 1’s behalf because German Bank 1’s research showed that Iranian Controlled Company 1 was “controlled from Iran.” And in June 2012, a BNP Paribas Paris

compliance officer noted that Iranian Controlled Company 1 was sending payments from its account at BNP Paribas Paris to its account at an Indian bank (“Indian Bank 1”) with “known links to Iran.” Nevertheless, despite these warnings—and despite claiming to be cooperating fully with the Government’s investigation into sanctions violations—BNP continued to process U.S. dollar transactions for Iranian Controlled Company 1 until November 2012.

1816. From December 2011, when U.K. Bank 1 blocked the payment involving Iranian Controlled Company 1 and in doing so put BNP on notice of the impermissibility of the transactions, through November 2012, when the transactions ended, BNP knowingly, intentionally and willfully processed a total of approximately \$586.1 million in transactions with Iranian Controlled Company 1, in violation of U.S. sanctions against Iran.

1817. BNP engaged in significant transactions with other sanctioned oil-and-gas companies in addition to Iranian Controlled Company I. In 2009, for example, BNP knowingly, intentionally, and willfully processed approximately \$100.5 million in USD payments involving an Iranian oil company following the revocation of the U-Tum Exemption, in violation of U.S. sanctions. The payments were in connection with six letters of credit issued by BNP that financed Iranian petroleum and oil exports—and the payments were made even after compliance personnel at BNP Paribas Paris alerted employees within BNP’s trade finance group that the USD payments associated with these letters of credit “are no longer allowed by American authorities.”

1818. BNP engaged in this conduct despite knowing, almost from the outset, that it was illegal to do so. As early as June 2003, BNP issued a “general procedure” that pertained to “Financial Embargoes,” which stated that “US financial embargoes apply within the US territory, to any US national or resident and to any transaction in US Dollar.” In addition, on several

occasions during the period covered by the bank's internal review, BNP sought external legal advice regarding its sanctions-related business, and specifically with regard to processing transactions on behalf of or involving sanctioned parties through the United States. Though not always consistent, the legal advice that BNP received described OFAC's comprehensive sanctions and explained why BNP should be careful in its business that involved parties subject to OFAC sanctions. Several BNP entities developed procedures or utilized payment practices that contravened the bank's June 2003 "general procedure" and processed thousands of transactions to or through the United States in violation of U.S. economic sanctions programs against Sudan, Iran, Cuba, and Burma.

1819. When a Dutch bank (ABN Amro) reached a settlement with United States regulators in 2005 for similar avoidance-of-sanctions practices to those conducted by BNP, the Head of Ethics and Compliance North America for BNP stated in an email "the dirty little secret, isn't so secret anymore, oui?"

1820. In early 2010, the New York County District Attorney's Office and the DOJ jointly approached BNP regarding its involvement in transactions with sanctioned entities, such as the sanctioned Iranian entities. Despite agreeing to commence an internal investigation into its compliance with U.S. sanctions and cooperate fully with U.S. and New York authorities, BNP continued to process these transactions on behalf of Iranian Controlled Company 1.

1821. BNP also provided access to substantial amounts of USD for sanctioned Sudanese entities, including those tied to Osama Bin Laden and al Qaeda. From at least November 1997 through in or around 2012, BNP conspired with Sudan, the Central Bank of Sudan, Al Shamal Islamic Bank, and al Qaeda to avoid OFAC sanctions that were put in place to deter, disrupt, and defeat terrorist activities. BNP maintained USD-denominated correspondent accounts for several

Sudanese banks, including four banks that OFAC identified as SDNs. From 2005 to 2009 alone, BNP processed at least 2,663 electronic funds transfers in the aggregate amount of \$8,370,372,624 to or through financial institutions located in the United States in apparent violation of U.S. sanctions on Sudan.

1822. After other banks stopped doing illegal business with Sudan, Sudan and Sudanese banks began requesting assistance from European banks to defeat the sanctions. For example, on November 9, 1997, one of Credit Lyonnais (Suisse) S.A.'s Sudanese institutional clients "sent a Telex message to all of its correspondents (including [Credit Lyonnais]) informing the banks of the sanctions imposed against Sudan and requested its correspondents 'not to [] channel such transactions by intermediation of any U.S.A. bank, including banks domiciled in the U.S.A. territory, U.S.A. banks overseas branches and subsidiaries [or the] [a]ffiliates of[a] U.S.A. bank incorporated outside the United States.'"

1823. BNP stepped in and, in 1997, effectively acted as Sudan's central banker for USD—BNP agreed to become Sudan's sole correspondent bank for one of Sudan's government banks. Without BNP providing USD, as the U.S. government found at BNP's criminal sentencing, Sudan and its related entities "would not have had access to the US dollar markets."

1824. BNP knew that Sudan had assisted al Qaeda prior to entering into the conspiracy. Despite that knowledge, BNP decided to become their sole correspondent bank in Europe, allowing it access to the U.S. financial market.

1825. All or nearly all major Sudanese banks had USD accounts with BNP Paribas Geneva. In addition to processing USD transactions, by or in 2000, BNP Paribas Geneva also developed a business in letters of credit for the Sudanese banks. Due to its role in financing Sudan's export of oil, BNP Paribas Geneva took on a central role in Sudan's foreign commerce

market. By 2006, letters of credit managed by BNP Paribas Geneva represented approximately a quarter of all exports and a fifth of all imports for Sudan. Over 90% of these letters of credit were denominated in USD. In addition, the deposits of a Sudanese Government Bank at BNP Paribas Geneva represented about 50% of Sudan's foreign currency assets during this time period.

1826. For example, soon after the imposition of U.S. sanctions against Sudan in 1997, BNP Paribas Geneva established account relationships with a network of nine unaffiliated regional banks located in Africa, Europe and the Middle East, some with no other business purpose than to clear payments for Sudanese clients. The accounts with the Regional Banks were created and established to provide a means to circumvent U.S. sanctions.

1827. Specifically, BNP utilized the Regional Banks in a two-step process designed to enable BNP's Sudanese clients to evade U.S. sanctions. In the first step, a Sudanese bank seeking to move USD out of Sudan transferred funds internally within BNP Paribas Geneva to an account specifically maintained by a Regional Bank to facilitate USD transfers from Sudan. In the second step, the Regional Bank transferred the money to the Sudanese bank's intended beneficiary through a U.S. bank without reference to the Sudanese bank. As a result, it appeared to the U.S. bank the transaction was coming from the Regional Bank rather than a Sudanese bank.

1828. In order to further disguise the true nature of the Regional Bank transactions, employees at BNP Paribas Geneva frequently worked with the Regional Banks to wait between one and two days after the internal transfer before making a dollar-for-dollar, transaction-by-transaction, clearing of funds through the United States, artificially delinking the U.S. transfer of funds from the prior transfer involving the Regional Banks so that financial institutions in the

United States and U.S. authorities would be unable to link the payments to the involved sanctioned party.

1829. In 2006 and 2007 alone, for example, BNP processed at least approximately \$6.4 billion through the United States on behalf of Sudanese sanctioned entities, including approximately \$4 billion on behalf of a financial institution owned by the government of Sudan. BNP processed these transactions even though internal emails showed BNP employees expressing concern about the bank's assisting the Sudanese government in light of its role in supporting international terrorism and committing human rights abuses during the same time period. Indeed, in March 2007, a senior compliance officer at BNP wrote to other high-level compliance and legal employees reminding them that certain Sudanese banks with which BNP dealt "play a pivotal part in the support of the Sudanese government which . . . has hosted Osama Bin Laden and refuses the United Nations intervention in Darfur."

1830. BNP's compliance personnel allowed these transactions to occur because the bank was earning significant money from them. BNP's senior compliance personnel agreed to continue the Sudanese business and rationalized the decision by stating that "the relationship with this body of counterparties is a historical one and the commercial stakes are significant. For these reasons, Compliance does not want to stand in the way."

1831. BNP also transacted illegal business with Al Shamal Islamic Bank, a Sudanese bank that received at least \$50 million in funding from Osama bin Laden in the 1990 time period. Al Shamal knowingly and intentionally provided financial services to al Qaeda, including maintaining and servicing al Qaeda bank accounts, including accounts for Osama bin Laden.

1832. Al Shamal held a correspondent bank account at United European Bank, a subsidiary of BNP. BNP and/or United European Bank continued its facilitation of Al Shamal

transactions even after public reporting of its ties to al Qaeda following the 1998 East African Embassy Attacks.

1833. BNP used a number of methods, in addition to the two-step approach described above regarding Sudan, to conceal these illegal transactions from other financial institutions and law enforcement.

1834. BNP internally published manuals instructing employees to cover payment messages being sent through the BNP Paribas New York headquarters to reflect only “the receiving institution (and not the Iranian beneficiary institution!)” As a result, this caused the BNP Paribas New York headquarters to be incapable of maintaining proper records of USD transactions cleared through that institution, and these transactions to go unnoticed by United States regulators.

1835. From as early as 1995 through at least 2007, BNP circulated memoranda among its operations staff with the blanket directive for USD transactions involving Iran: “[d]o not stipulate in any case the name of the Iranian entities on messages transmitted to American banks or to foreign banks installed in the U.S.”

1836. BNP staff in the New York headquarters knew they were operating without adequate legal and compliance authority to ensure activities conducted by BNP outside of the United States, but directed at the United States, complied with New York and United States sanctions law in dealing with prohibited countries, such as Iran.

1837. For example, in 2006, when questioning whether BNP practices with respect to whether an internal group at BNP dealing with energy and commodities exports ran the risk of circumventing United States sanction law, an employee described “a practice exists which consists in [sic] omitting the Beneficiaries/Ordering party’s contact information for USD

transactions regarding clients from countries that are under U.S. embargo: Sudan, Cuba, Iran. This avoids putting BNP NY in a position to uncover these transactions, to block them, and to submit reports to the regulators.”

1838. The highest levels of compliance authorities at BNP Paribas New York were aware of and accepted the widespread practice of amending, omitting or stripping information from USD payment transactions for the benefit of sanctioned countries, such as Iran.

1839. BNP Geneva also intentionally implemented a “solution” to the problems presented by United States sanction law by using other, non-BNP financial institutions located in the United States to conduct its knowingly improper USD transactions on behalf of sanctioned countries, such as Iran.

1840. Another scheme BNP used to evade sanctions and deceive regulators was to shift its illicit USD transactions from its New York Branch to another unaffiliated U.S. bank—once BNP began to come under regulatory pressure for unsatisfactory compliance procedures. BNP engaged in this strategy after authorities identified bank-wide failures in BNP’s AML requirements.

1841. Based on this illegal conduct, BNP pled guilty in the United States District Court for the Southern District of New York to one count of Conspiracy to Violate the IEEPA (50 U.S.C. § 1702, 1705) and the Trading with the Enemy Act (50 U.S.C. §§ 3, 5, 16).<sup>182</sup>

1842. BNP also entered into a Consent Order with the DFS based on its illegal banking activities with sanctioned Countries, including Iran. In particular, BNP pled guilty to one count

---

<sup>182</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Guilty Plea entered into by BNP Paribas on or about July 10, 2014, as if fully set forth herein.

of falsifying business records in the first degree (New York Penal Law § 175.10) and one count of conspiracy.<sup>183</sup>

1843. Further, BNP entered into a Settlement Agreement with OFAC for violations of a number of federal banking laws, including the breach of 31 C.F.R. § 560.204, prohibiting the exportation or re-exportation of services from the United States to Iran.<sup>184</sup>

1844. As a result of the above transgressions targeting the United States financial system for the benefit of Iranian entities, BNP pled guilty to and voluntarily entered into multi-faceted, agreements with both the DOJ, the United States Department of the Treasury and the state of New York that required forfeiture of significant assets, extensive reshaping of their internal compliance departments and wide-ranging monitoring by United States law enforcement.

1845. As required by its guilty plea in the United States District Court for the Southern District of New York, BNP agreed to:

- a) Forfeit \$8,833,600,000 to the United States;
- b) The entry to a money judgment against it in that amount;
- c) Be subject to judicial process in the United States for determining the locations of such funds, if not paid;
- d) Be subject to the continuing jurisdiction of the United States to enforce the terms of its guilty plea and forfeiture;
- e) Be subject to a term of probation supervised by the United States for a term of five years, including:

---

<sup>183</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Settlement Agreement entered into between BNP Paribas and the U.S. Department of Treasury on or about June 30, 2014, as if fully set forth herein.

<sup>184</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order entered into between BNP Paribas and the New York Department of Financial Services on or about June 30, 2014, as if fully set forth herein.

- i. the standard terms of probation for all criminals convicted in the United States, and;
- ii. compliance with all terms of the agreement entered into by BNP with the State of New York.

1846. As a result of the guilty plea entered into with the State of New York, BNP agreed to:

- a) Pay over three billion dollars of the amount agreed to be forfeited by its agreement with the United States to the State of New York in the form of reparations and restitution;
- b) Suspend its USD clearing services through its New York headquarters starting January 1, 2015 for a period of one year;
- c) Prohibit, for a period of twenty-four months, USD clearing unaffiliated third party banks in New York and London;
- d) Not to take any action to avoid or circumvent these suspensions;
- e) Extend for an additional two years the tenure of a previously agreed to Independent Consultant (through a prior agreement with the state of New York) who is on-site at the BNP Paribas New York headquarters to review BNP compliance with United States regulations affecting transactions with sanctioned countries, such as Iran. The Independent Consultant will also:
  - i. Oversee BNP's remediation efforts to streamline USD transactions process through the BNP Paribas New York headquarters; and
  - ii. Monitor compliance with the previously referenced suspension of USD activities.
- f) Terminate 13 executives with responsibility for conducting or tacitly condoning the failure of BNP to comply with United States law regarding transactions with sanctioned entities, such as Iran;
- g) Discipline an additional 32 employees who were also responsible for circumventing United States sanction law, with such discipline including cuts in compensation, remedial training and warnings;
- h) Not hire, retain or indirectly retain any of the terminated employees; and

- i) To be prosecuted to the full extent of United States law in the event it breached the agreement with the State of New York.

1847. As a result of the Settlement Agreement entered into between BNP and OFAC, BNP agreed:

- a) Provide all reports generated as a result of its other settlement with governmental entities to the United States Department of the Treasury; and
- b) Pay up to \$963,619,900 to the United States in the event lesser amounts were assessed by other governmental entities as a result of BNP's improper conduct.

## **7. Standard Chartered Bank's Participation in the Conspiracy**

1848. SCB agreed to, and participated in, the Conspiracy.

1849. Beginning by at least 2001 and continuing through at least 2007, SCB had a continuous, ongoing relationship with Iran and its Agents and Proxies.

1850. SCB "conspired with its Clients to route nearly 60,000 different USD payments through SCB's New York branch after first stripping information from wire transfer messages used to identify sanctioned countries, individuals and ("wire stripping")."<sup>185</sup>

1851. For nearly a decade, SCB programmatically engaged in deceptive and fraudulent misconduct in order to move at least \$250 billion in approximately 59,000 transactions through its New York branch on behalf of client Iranian financial institutions that were subject to U.S. economic sanctions, including Iranian sanctioned entities, and then covered up its transgressions. These institutions included no less than the Central Bank of Iran/Markazi, as well as Bank Saderat and Bank Melli, both of which are also Iranian State-owned institutions. These transactions generated at least hundreds of millions in fees for SCB.

---

<sup>185</sup> New York State Department of Financial Services, *In re STANDARD CHARTERED BANK, NEW YORK BRANCH, New York, New York, Order Pursuant to Banking Law § 39*, <http://www.dfs.ny.gov/about/ea/ea120806.pdf> (last visited Oct. 15, 2017).

1852. A critical component of the deal between SCB and the Central Bank of Iran/Markazi was the timing of \$500 million in daily USD payments. A senior manager of SCB's Iranian business noted that "the most important aspect to the Central Bank of Iran/Markazi of this relationship with Standard Chartered Bank" was SCB's "willingness to pay away funds in advance of receipts (intraday up to USD 200m)." He stressed that providing rapid USD payments for the Central Bank of Iran/Markazi "could lead to increased business activity with [other Iranian] banks."<sup>186</sup>

1853. The senior manager of SCB's Iranian business was correct. For the next "10 years SCB [Standard Chartered Bank] schemed with Iran and hid from regulators roughly 60,000 secret transactions, involving at least \$250 billion, and reaping Standard Chartered Bank hundreds of millions of dollars in fees. SCB's actions left the U.S. financial system vulnerable to terrorists, weapons dealers, drug kingpins and corrupt regimes, and deprived law enforcement investigators of crucial information used to track all manner of criminal activity."<sup>187</sup>

1854. Defendants SCB provided, *inter alia*, trade-finance, Eurodollar and foreign exchange banking services to Iranian clients starting in or about 1993. At some point thereafter, SCB began formulating plans to participate in and further the Conspiracy with Iran.

1855. SCB utilized such schemes to cloak the dollar clearing activities of Iran's Agents and Proxies and thereby shield those transactions from regulatory scrutiny. During the Relevant Period, OFAC required U.S. financial institutions to filter all dollar clearing transactions so as to identify those involving sanctioned entities, and then to freeze suspect transactions pending investigation. This system could (a) delay transaction processing; (b) require that OFAC be

---

<sup>186</sup> *Id.*

<sup>187</sup> New York State Department of Financial Services – Order Pursuant to Banking Law 39, at 1.

advised of information surrounding a transaction; and (c) ultimately result in the rejection of a transaction. SCB therefore wire-stripped to ensure the automatic and unobstructed clearance of Iranian transactions in New York.

1856. For example, on June 1, 1995, SCB's General Counsel wrote an e-mail advising SCB's regulatory compliance staff: "if SCB London were to ignore OFAC's regulations AND SCB NY were not involved in any way & (2) had no knowledge of SCB Londons [sic] activities & (3) could not be said to be in a position to control SCB London, then IF OFAC discovered SCB London's [sic] breach, there is nothing they could do against SCB London, or more importantly against SCBNY." The SCB General Counsel also instructed that a memorandum containing this plan was "highly confidential & MUST NOT be sent to the US." In the ensuing years, SCB actively conspired with the CBI, Bank Melli Iran, Bank Saderat Plc's predecessor (Iran Overseas Investment Bank) and many other entities to assist Iran evade U.S. sanctions.

1857. SCB's role in the Conspiracy grew dramatically in early 2001, when the CBI approached SCB to act as the Central Bank of Iran's recipient bank for USD proceeds from daily oil sales made by the NIOC in the Eurodollar market. An e-mail dated February 19, 2001, from SCB's Head of Inbound Sales, Institutional Banking, characterized the CBI's solicitation of Standard Chartered as "very prestigious" because "in essence, SCB would be acting as Treasurer to the CBI ..." Thus, SCB was knowingly laundering billions of dollars in violation of multiple U.S. laws for the benefit of, among others, the IRGC.

1858. In a follow up e-mail dated March 23, 2001, SCB's Group Legal Advisor wrote to its Product Manager, Corporate & Institutional Banking and its General Counsel (the e-mail was also forwarded to SCB's Group Head of Audit) that "our payment instructions [for Iran's Agents and Proxies] should not identify the client or the purpose of the payment."

1859. SCB and the CBI quickly developed operating procedures for USD funds transfers to mask the involvement of Iranian entities in payment orders sent to SCB's New York branch.

1860. When the beneficiary bank of a CBI Eurodollar payment transaction was an Iranian bank, SCB-London would send a SWIFT-NET MT 100 or MT 103 to the beneficiary bank's non-U.S., non-Iranian correspondent bank with full details of the Iranian beneficiary bank, and a separate MT 202 to SCB's New York branch with no mention of the Iranian beneficiary bank.

1861. In fact, SCB-London set up routing rules within its payment system to route all incoming SWIFT-NET messages from the CBI to a repair queue, meaning the payments were subject to manual review and processing by wire operators, to prevent SCB - London from automatically processing outbound payment instructions for clearance and settlement in the United States with a reference to the CBI in the payment message.

1862. SCB - London's payment processing team initially instructed the CBI to insert Standard Chartered Bank - London's SWIFT-NET Bank Identification Code ("BIC") address (identified as SCBLGB2L) in field 52 (ordering institution) of its incoming payment order messages so that SCB's payment system would not populate that field with the CBI's SWIFT-NET BIC address (identified as BMJIIRTH).

1863. When the CBI failed to remove its BIC address and insert SCB's BIC address into each SWIFT-NET message, Standard Chartered Bank - London wire operators would manually change field 52 to reference SCB - London's BIC in order to mask the CBI's involvement in the payments. SCB's willingness to further the Conspiracy in this manner attracted more illicit business.

1864. As early as February 2002, several additional Iranian banks approached SCB - London to discuss the possibility of opening new accounts.

1865. SCB - London's Legal, Compliance, and Cash Management groups identified the need for written procedures for the operation of these additional Iranian banks' dollar-denominated accounts.

1866. SCB's central role in the Conspiracy was memorialized in an internal memorandum regarding SCB's procedures for processing payments sent through the United States from the Iranian banks. The document was entitled "Standard Chartered Bank Cash Management Services UK - Quality Operating Procedure: Iranian Bank Processing." It was first issued to SCB London staff on February 20, 2004, and included detailed instructions regarding the omission of the Iranian remitting bank's BIC:

Ensure that if the field 52 of the payment is blank or that of the remitting bank that it is overtyped at the repair stage to a "." (Note: if this is not done then the Iranian Bank SWIFT code may appear - depending on routing - in the payment message being sent to SCB's New York branch).

1867. In addition to inserting a "." in field 52, the memorandum also instructed staff to use cover payments to process Iranian bank payments, which resulted in SCB London omitting any reference to the involvement of Iranian beneficiaries or beneficiary banks in SWIFT-NET payment order messages sent to SCB's New York branch.

1868. This element of the Conspiracy was particularly important to Defendant Bank Saderat which repeatedly served as the Reimbursing Bank on Letters of Credit for other Iranian banks that were financing various illegal, sanctions-evading transactions on behalf of the IRGC and MODAFL through the United States.

1869. Approximately 60,000 payments related to Iran, totaling \$250 billion, were eventually processed by SCB as part of the Conspiracy.

1870. An e-mail dated March 9, 2003, from SCB's Head of Transactional Banking Solutions, UK/Europe Corporate & Institutional Banking to several of SCB's wholesale bank business managers indicates that Standard Chartered Bank learned that another bank was "withdrawing their services" with one of its Iranian client banks "primarily for reputational risk reasons."

1871. In a memorandum accompanying the news of the aforementioned bank's reduction in Iranian business entitled "Summary of the Risks/Issues to be Addressed with Regard to Iranian Bank USD Clearing that Require Management Direction from Middle East Senior Management Team," the risks posed by additional Iranian business that might "trigger an action" from OFAC, "leaving SCB exposed, with potential reputational damage" were considered, but ultimately rejected in favor of pursuing additional Iranian business.

1872. An October 15, 2003 e-mail from SCB's Manager, Cash Management Services, London to SCB's Product Manager, Corporate & Institutional Banking and its Head of Cash Management Services, UK (forwarded to SCB's Head of Legal & Compliance, Americas and Head of Legal for Corporate & Institutional Banking) outlined how the CBI was instructed to "send in their MT 202's with a [SCB London's business identifier code] as this is what we required them to do in the initial set up of the account. Therefore, the payments going to NY do not appear to NY to have come from an Iranian Bank."

1873. When SCB anticipated that its business with the Iranian Bank co-conspirators, including Defendant Bank Saderat, would grow too large for SCB employees to manually "repair" the payment order messages for New York bound wire transfers, SCB automated the process by building an electronic repair system with "specific repair queues" for each Iranian client.

1874. SCB's payment "Quality Operations Procedures" manual contained instructions on how to manually "repair" or "over-type field 52 as [SCB London]" in SWIFT-NET MT 202 payment message fields to hide CBI's role as originator of the MT 202 cover payment transactions SCB was processing through New York in USD funds.

1875. In October 2004, SCB consented to a formal enforcement action and executed a written agreement with the N.Y. State Banking Department and the FRBNY, which required SCB to adopt sound Bank Secrecy Act and AML practices with respect to foreign bank correspondent accounts (the "Written Agreement").

1876. The Written Agreement arose as a result of identified flaws in AML risk controls at SCB's New York branch and it required SCB to adopt sound AML practices with respect to foreign bank correspondent accounts.

1877. The Written Agreement also required SCB to hire an independent consultant to conduct a retrospective transaction review for the period of July 2002 through October 2004.

1878. The review was intended to identify suspicious activity involving accounts or transactions at, by, or through SCB's New York branch.

1879. SCB failed to inform the N.Y. State Banking Department and the Federal Reserve Board of New York that its London and Dubai operations were secretly clearing hundreds of billions of dollars through SCB's New York branch at the same time that it was promising to reform its AML practices.

1880. SCB also failed to inform the N.Y. State Banking Department and the Federal Reserve Board of New York that its London, Dubai, Bahrain, Singapore and Hong Kong operations were secretly helping MODAFL and the IRGC evade U.S. sanctions at a time when they were illegally acquiring a wide range of U.S. equipment and technologies, including

components for IEDs and EFPs used to kill and maim Coalition Forces in Iraq, including Plaintiffs.

1881. SCB retained Deloitte to conduct the required “independent” review and to report its findings to the regulators.

1882. On August 30, 2005, and again on September 17, 2005, Deloitte provided SCB confidential historical transaction review reports that Deloitte had prepared for two other major foreign banking clients that were under investigation for OFAC violations and money laundering activities.

1883. Deloitte’s reports contained detailed and highly confidential information concerning foreign banks involved in illegal USD clearing activities.

1884. SCB then asked Deloitte to delete from its draft “independent” report any reference to certain types of payments that could ultimately reveal SCB’s illegal Iranian-related practices.

1885. In an e-mail dated October 1, 2005, SCB’s Group Head of Legal & Compliance, Wholesale Bank, forwarding the Quality Operating Procedure to SCB’s Group Head of Compliance and Regulatory Risk, its Group Legal Advisor and its Head of Financial Crime Risk Systems and Monitoring, observed that “read in isolation, is clearly ... designed to hide, deliberately, the Iranian connection of payments.”

1886. A few days later, in an e-mail dated October 8, 2005, Deloitte’s Global Leader of AML/Trade Sanctions Division wrote to SCB’s Head of Compliance, that Deloitte had “agreed” to accede to SCB’s request that Deloitte delete from its draft “independent” report any reference to certain types of payments that could ultimately reveal SCB’s illegal Iranian U-turn practices

because “this is too much and too politically sensitive for both SCB and Deloitte. That is why I drafted the watered-down version.”

1887. In a December 1, 2005 internal memorandum entitled “Project Gazelle,” SCB’s Group Head of Compliance and Regulatory Risk and its CEO in the UAE wrote to SCB’s Group Executive Director for Risk and its Group Head of Global Markets, acknowledging that SCB repair procedures for U-turn exemption transactions did “not provide assurance that it does not relate to a prohibited transaction, and therefore SCB NY is exposed to the risk of a breach of sanctions.”

1888. SCB intentionally withheld material information from New York and Federal regulators in its effort to service Iran’s Agents and Proxies. SCB carefully planned its deception and was apparently aided by its consultant Deloitte, which intentionally omitted critical information in its “independent report” to regulators. This ongoing misconduct was especially egregious because – during a key period between 2004 and 2007 – SCB’s New York branch was subject to a formal supervisory action by the Department and the FRBNY for other regulatory compliance failures involving the Bank Secrecy Act, AML, and OFAC regulations.

1889. In short, SCB operated as a rogue institution. By 2006, even the New York branch was acutely concerned about the bank’s Iran dollar-clearing program. In October 2006, SCB’s CEO for the Americas sent a panicked message to the Group Executive Director in London. “Firstly,” he wrote, “we believe [the Iranian business] needs urgent reviewing at the Group level to evaluate if its returns and strategic benefits are... still commensurate with the potential to cause *very serious or even catastrophic reputational damage* to the Group.” His plea to the home office continued: “[s]econdly, there is equally important potential of risk of subjecting

management in US and London (e.g. you and I) and elsewhere to personal reputational damages and/or *serious criminal liability*.”<sup>188</sup>

1890. SCB’s obvious contempt for U.S. banking regulations was succinctly and unambiguously communicated by SCB’s Group Executive Director in response. As quoted by an SCB New York branch officer, the Group Director caustically replied: “You f---ing Americans. Who are you to tell us, the rest of the world, that we’re not going to deal with Iranians.”<sup>189</sup>

1891. According to SCB, its success as a bank is due in part because it is “trusted worldwide for upholding high standards of corporate governance.” SCB prides itself for having a “distinctive culture and values [that] act as a moral compass.” It boasts “openness” as one of its “core values” and claims to aspire to be “trustworthy.” It also markets itself to clients and the investing public as “always trying to do the right thing.”<sup>190</sup>

1892. A February 23, 2006 internal memorandum entitled “Iranian Business” sent from SCB’s General Counsel to SCB’s Audit and Risk Committee confirmed SCB’s continued recognition the Conspiracy was expressly designed to enable Iran and other co-conspirators (including Defendant Bank Saderat) to evade U.S. detection of their transactions and confirmed that “certain US\$ clearing transactions handled in London were processed with the name of the Iranian Bank excluded or removed from the ‘remitter field’” despite the “requirement that due diligence in respect of ‘U-turn’ payments should be undertaken by our office in New York.”

---

<sup>188</sup> *Supra* n. 6.

<sup>189</sup> Note of Interview with SCB’s Head of Cash Management Services (2002-2005), Head of Compliance (2005-2007) at the New York branch, SCB INT 0004733-4734.

<sup>190</sup> See <http://www.standardchartered.com> (last visited Oct. 15, 2017).

1893. In September 2006, New York State regulators requested that SCB provide them with statistics on Iranian U-turns SCB handled, including the number and dollar volume of such transactions for a 12-month period.

1894. In response, SCB searched its records for 2005 and 2006. In a September 26, 2006 email from SCB's Project Manager for the Lookback Review to SCB's Head of Cash Management Services (2002-2005) and Head of Compliance (2005-2007) at SCB's New York branch, SCB's Head of Operations and Head of Cash SCB identified 2,626 transactions totaling over \$16 billion (for Iranian banks).

1895. Faced with the prospect of disclosing billions of dollars in Iranian transactions SCB's New York branch's Head of Compliance was directed by his superiors at SCB to provide instead only *four days* of U-turn data to regulators; these four days were masquerading as a log covering two-years of transaction data.

1896. In 2007, SCB successfully convinced the N.Y. State Banking Department and FRBNY to lift their consent order on SCB based on the watered down Deloitte report and its other fraudulent disclosures.

1897. As noted above, from approximately January 2001 through 2007, SCB transferred at least \$250 billion through SCB's New York branch on behalf of the Iranian Bank co-conspirators, including Bank Melli Iran and the CBI, as well as Defendant Bank Saderat.

1898. SCB's New York branch processed approximately 60,000 wire transfers on behalf of the Iranian Bank co-conspirators, with roughly half the transactions originating with SCB's London office, and the other half with SCB's branch in Dubai, UAE.

1899. In early 2009, after being contacted by U.S. law enforcement authorities, SCB conducted yet another “internal investigation” into its OFAC sanctions screening procedures, business practices, and technology.

1900. Nonetheless, SCB’s New York branch was the conduit for at least 50 post-U.S. designation transactions on behalf of IRISL and its various front companies through June 2010.

1901. As of 2011, however, even after its internal investigation and open law enforcement investigations commenced in the U.S., the New York State Banking Department still found that SCB’s New York branch had:

- a) No documented evidence of investigation before the release of funds for transactions with parties whose names matched the OFAC-sanctioned list; and
- b) Outsourced SCB’s New York branch’s entire OFAC compliance process to Chennai, India, with no evidence of any oversight or communication between the Chennai and SCB’s New York branch.

1902. From at least 2001 to 2007, SCB illegally facilitated more than 1,300 Letters of Credit through stripping or cover payment methods that purposefully concealed the participation of Iranian counterparties in the transactions.

1903. Many of those Letters of Credit were issued for the benefit of Iran’s military/terror apparatus, facilitating and financing the IRGC’s, MODAFL’s and Hezbollah’s illegal acquisitions of materials and technologies, including materials unlawfully obtained from the United States and components for IEDs and EFPs used against Coalition Forces in Iraq.

1904. SCB knowingly facilitated and financed the illegal export to Iran of U.S.-manufactured, export-controlled defense and dual-use products worth tens of millions of dollars.

1905. These were acquired by various Iranian-controlled front companies on behalf of, *inter alia*, the following entities:

- a) Mahan Air;

- b) Four MODAFL subsidiaries: the AIO, the Iran Aircraft Industries, the IHSRC, and IAMIC;
- c) The Iran Power Development Company, MAPNA and Zener Electronics Services (an agent of Hezbollah);
- d) The NIOC and several of its subsidiaries; and
- e) Khoram Sanat Producing Co. – Iran.

1906. Mahan Air is a SDGT that, according to the U.S. government, (1) “facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq;” (2) “facilitated IRGC-QF arms shipments;” and (3) “transported personnel, weapons and goods on behalf of Hezbollah.”

1907. Mahan Air was also later identified as a major conduit to Iran of thousands of radio frequency modules recovered by Coalition Forces in Iraq from IED devices that were used to target, kill and maim U.S. and Coalition Forces.

1908. Similarly, MODAFL is the principal procurement arm of Iran’s military and terror apparatus.

1909. The MAPNA group is also a key component of MODAFL and the IRGC’s procurement chain.

1910. Abbas Aliaabadi, Chairman of MAPNA International FZE and President of the MAPNA Group, is a former member of the Iranian Ministry of Construction Jihad and of the Iranian Air Force. Aliaabadi was also a key member of the Ministry of Culture & Islamic Guidance instrumental in the creation of Hezbollah and has close links to the IRGC.

1911. During the Relevant Period, the NIOC was not only controlled by the IRGC but the company also served as the lifeblood of the Iranian regime’s illicit financing activities, providing it with access to billions of dollars in oil and natural gas revenues that enabled the IRGC to gain access (through the Conspiracy) to the global financial system.

1912. SCB knowingly conspired with Iran to facilitate illicit trade for all of these entities in violation of U.S. law, thereby substantially assisting Iran in its criminal (and specifically terrorist) conduct in Iraq. The foreseeable consequence of that assistance was to enable Iran, the IRGC and Hezbollah to kill or wound, or try to kill, or conspire to kill more Americans in Iraq.

1913. At all relevant times, SCB was fully aware of both the Iran Trade Regulations and the Export Administration Regulations, the U.S. State Department's United States Munitions List, and their many restrictions.

1914. Between 2000 and 2006, SCB facilitated LCs for the benefit of Mahan Air totaling more than \$120 million.

1915. The Treasury Department made the following findings regarding Mahan Air in designating the organization:

Mahan Air also facilitated the covert travel of suspected IRGC-QF officers into and out of Iraq by bypassing normal security procedures and not including information on flight manifests to eliminate records of the IRGC-QF travel. Mahan Air crews have facilitated IRGC-QF arms shipments. Funds were also transferred via Mahan Air for the procurement of controlled goods by the IRGCQF. In addition to the reasons for which Mahan Air is being designated today, Mahan Air also provides transportation services to Hezbollah, a Lebanon-based designated Foreign Terrorist Organization. Mahan Air has transported personnel, weapons and goods on behalf of Hezbollah and omitted from Mahan Air cargo manifests secret weapons shipments bound for Hezbollah.

1916. Mahan Air also transported to Iran thousands of radio frequency modules illegally imported by OPTO Electronics in Singapore, NEL Electronics PTE Ltd. and Corezing International PTE Ltd. from the United States.

1917. These modules were recovered by Coalition Forces in Iraq from IED devices that were used to target U.S. and Coalition Forces.

1918. The modules had encryption capabilities and a particularly long range that allowed Special Groups operatives to operate them across significant distances.

1919. In 2008, Mahan Air transported the IED components from Singapore and Thailand to Tehran, Iran.

1920. Under Secretary of Commerce Eric L. Hirschhorn described this supply chain as “egregious conduct by... foreign companies and individuals who have endangered the lives of U.S. and coalition forces in Iraq.”

1921. Five LCs facilitated by SCB listed Mahan Air as the “Applicant” and involved the illegal acquisition of materials ranging from aviation parts to a U.S. shipment of an Airbus A320.

1922. The Issuing Banks for the LC included Defendant Bank Saderat, Bank Melli Iran, and Bank Sepah.

1923. SCB’s New York branch served as the clearing bank for these Letters of Credit.

1924. Furthermore, in another transaction, Mahan Air was the listed Beneficiary of a \$21 million dollar LC facilitating the leasing of several second-hand Airbus A320s from Europe.

1925. In facilitating these trade-finance transactions, often for explicitly “Non-EAR 99” goods of U.S. origin – i.e. products on the Commerce Control List, SCB knew that it was (1) working with Iranian banks, (2) concealing the Iranian connection to the trade-finance and Eurodollar transactions and (3) facilitating the unlawful delivery of these U.S. export-controlled parts or products to Iranian entities in Iran.

1926. For at least two transactions facilitated on behalf of Mahan Air (including one for export-controlled goods of entirely U.S. origin), Credit Suisse in Zurich facilitated the payment on the LC to SCB, Dubai, and on at least one of those transactions, the payment was routed by

Defendant Credit Suisse in Zurich through New York on behalf of Bank Melli in the UAE with the transaction being cleared and settled in USD funds by SCB's New York branch.

1927. On one occasion, Mahan Air purchased an Airbus (aircraft) using Blue Sky Aviation as its intermediary. SCB Dubai provided the nearly \$30 million to Blue Sky for the purchase, and Bank Sepah (Iran) guaranteed the payment through a re-payment made by Defendant and co-conspirator Credit Suisse on its behalf in 2006.

1928. The front companies listed as beneficiaries of the LCs facilitated by SCB included Sirjanco Trading LLC ("Sirjanco") and Blue Sky Aviation Co FZE ("Blue Sky Aviation"), both later designated by the U.S. Treasury as SDGTs, in part, because of the illegal sanctions evading conduct facilitated and enabled by SCB.

1929. Hamidreza Malekouti Pour served simultaneously as the Regional Manager for Mahan Air in the UAE, and Managing Director of Sirjanco and Blue Sky Aviation – effectively demonstrating how these companies are all part of the same IRGC supply chain. Pour has also been designated as an SDGT for, *inter alia*, supplying equipment to the IRGC-QF.

1930. When designated by the U.S. Treasury Department in 2013 as a SDGT, Sirjanco was described as "a United Arab Emirates-based company designated pursuant to E.O. 13224 for acting for or on behalf of Mahan Air. Sirjanco was established specifically to serve as a financial front for Mahan Air. Sirjanco has also served as a front for Mahan Air's acquisition of aircraft. Additionally, Iran's IRGC-QF has used Sirjanco to procure sanctioned goods."

1931. A 2005 LC facilitated by SCB listed Mahan as the Applicant, and Sirjanco as the beneficiary, for a total of \$32,500,000.

1932. Bank Melli financed the payment through Defendant and co-conspirator Credit Suisse, which sent the payment order through New York (clearing and settling in USD funds through SCB’s New York branch).

1933. The payment was made by SCB, Dubai to Sirjanco’s account with Bank Saderat, Dubai.

1934. At least two other Letters of Credit facilitated by SCB listed Mahan Air as the Applicant, and Blue Sky Aviation as the Beneficiary, for a total of over \$60,000,000. All told, between 2000 and 2006, SCB facilitated at least 11 Letters of Credit for the “Blue Sky Group” for a total of more than \$125 million.

1935. When the U.S. Treasury Department designated Blue Sky Aviation in 2014, it described it as “a UAE-based company that is owned or controlled by Mahan Air and acts for or on behalf of the airline.”

1936. Blue Sky Aviation’s primary function has been to serve as a payment channel for Mahan Air to obscure the origination of funds. Mahan Air has used Blue Sky Aviation to make payments to oil suppliers, and purchase aircraft, engines, and parts.”

1937. In sum, SCB was vital to Mahan Air’s continued operations and its ability to facilitate travel by IRGC-QF officers and arms shipments in and out of Iraq, transport IED technologies into Iraq as well as transit personnel, weapons and goods on behalf of Hezbollah, which helped facilitate terrorist attacks in Iraq during the Relevant Period.

1938. While neither Mahan Air nor Blue Sky Aviation was designated as a terrorist organization at the time the LCs identified above were financed, SCB engaged in criminal conduct in furtherance of the Conspiracy in order to aid these IRGC supply chain entities to evade U.S. sanctions knowing that its own conduct was illegal.

1939. At the time it agreed to engage in overt acts in furtherance of the Conspiracy, SCB knew that Mahan Air was seeking to illegally acquire U.S. export-controlled defense and dual-use materials and that Mahan Air was using front companies to do so.

1940. In sum, SCB affirmatively chose to facilitate Iran's illegal conduct and provide material support to its terror apparatus, including Mahan Air, Blue Sky Aviation and Sirjanco. All of these entities were later designated as SDGTs in part because of the types of trade-finance and Eurodollar transactions facilitated by SCB. Iran's MODAFL operates the Iran Aviation Industries Organization, the AIO, and the DIO. MODAFL was designated by the United States on October 25, 2007.

1941. The AIO was designated on June 28, 2005 for weapons proliferation. SCB knowingly provided financing for both the AIO directly, and for three major sub-agencies of MODAFL's Iran Aviation Industries Organization: the Iran Aircraft Industries, the Iran Helicopter Support and Renewal Company ("IHSRC") a/k/a PANHA, and the Iran Aircraft Manufacturing Industrial Company ("IAMIC"). Support for any of these entities, as sub-agencies of MODAFL and the Iran Aviation Industries Organization, was not for legitimate agencies, operations or programs of Iran.

1942. In 2002, SCB facilitated a LC for MODAFL's Aerospace Industries Organization that cleared through SCB's New York branch valued at \$57,662 USD for the illegal purchase of U.S. export-controlled goods.

1943. That transaction was not for the benefit of any legitimate agencies, operations or programs of Iran. On numerous additional occasions, SCB illegally facilitated trade-finance and Eurodollar transactions on behalf of other MODAFL sub-agencies, including IAMIC.

1944. On September 17, 2008, the U.S. Treasury Department designated IAMIC, finding that it is:

owned or controlled by MODAFL, and also because it has provided support to the Iranian Revolutionary Guard Corps (IRGC). The IRGC, which was designated under Executive Order 13382 on October 25, 2007, is considered to be the military vanguard of Iran and has been outspoken about its willingness to proliferate ballistic missiles capable of carrying WMD. [IAMIC] utilizes its own facilities for the inspection, maintenance, repair overhaul research, development, and manufacture of military and civilian aircraft and related military logistic systems. [IAMIC] conducts research on, development of, production of, and flight operations for unmanned aerial vehicles (UAVs) in Iran. The IRGC utilizes the “Ababil” UAV, manufactured by [IAMIC]. [IAMIC] produces different variants of the Ababil UAV, which can be used for surveillance and attack. Farasakht Industries is a subsidiary of [IAMIC] that specializes in the manufacturing of various aerospace tools and equipment.

1945. Between 1998 and 2002, SCB facilitated ten LCs involving a company based in Malaysia (and with links to a same named company registered in the U.K.), Downtown Trading (“Downtown Trading”).

1946. The total value of these ten LCs involving Downtown Trading amounted to \$1,067,575.

1947. MODAFL-Iran Aviation Industries Organization’s subsidiary Iran Aircraft Industries was the Applicant on these LCs, i.e., the purchaser of the U.S. origin aircraft engine parts in question for seven of these transactions, while Downtown Trading was the reported Beneficiary.

1948. In most or all of these transactions, primarily those for 2002, Bank Sepah (Iran) served as the Issuing Bank, Bank Sepah (London) served as the Reimbursing Bank, SCB Dubai served as the Negotiating Bank, and SCB’s New York branch helped facilitate the transactions by serving as the Clearing Bank.

1949. With respect to at least four of these transactions, the U.S. aircraft parts were transported by Iran Air, later designated as “a commercial airline used by the IRGC and MODAFL to transport military related equipment.... Iran Air has provided support and services to MODAFL and the IRGC through the transport and/or transfer of goods for, or on behalf of, these entities.”

1950. Iran Aircraft Industries’ illegal procurements were often financed by Bank Sepah (as the Issuing Bank), but SCB in Dubai frequently served as the Negotiating Bank and SCB’s New York branch usually served as the Clearing Bank for these same trade-finance transactions, in at least one case paying Citibank in New York the fund due.

1951. Citibank then paid Maybank, Malaysia, which effected the ultimate payment to the Eurodollar account of Downtown Trading.

1952. SCB also facilitated similar LCs in USD funds for Downtown Trading after April 2005.

1953. In facilitating these transactions – 70% of which explicitly involved export-controlled “Non-EAR 99” goods of U.S. origin (i.e. products on the Commerce Control List) – SCB knew: (1) it was working with Iranian banks; (2) it was concealing the Iranian connection to the transactions; (3) it was facilitating the unlawful delivery of goods on the U.S. Commerce Control List to Iran’s military and/or the IRGC; and (4) these transactions were not for legitimate agencies, operations, or programs of Iran.

1954. Mac Aviation is an Irish trading company incorporated in 1993 that purported to engage in the purchase and sale of aircraft and helicopter parts.

1955. The company and its owners were indicted in 2008 for, among other things, violations of the IEEPA, the Iranian Transactions Regulations, and U.S. export controls.

1956. During the Relevant Period, Mac Aviation was a customer of SCB in London.

1957. According to the indictment, between June 2005 and July 2008 Mac Aviation solicited purchase orders from customers in Iran for U.S. origin aircraft parts and then forwarded these requests for the parts to U.S. companies.

1958. The indictment further alleges that Mac Aviation wired funds to banks in the U.S. as payment for these parts, and concealed from U.S. sellers the ultimate end-use and Iranian end-users of the purchased parts.

1959. The indictment also alleges that Mac Aviation caused the export of these parts from the U.S. to third countries, including Malaysia, before sending their shipments onward to Iran.

1960. At least one of those shipments, directed by Mac Aviation in February 2006, resulted in a shipment to be made from a firm called Microset Systems Sdn Bhd in Kuala Lumpur, Malaysia, to Sasadja Moavanate Bazargani in Tehran, Iran, an alter ego of Iran's DIO, which had been designated by Germany, the United Nations, and the United States as a procurer of unlawful weapons components beginning as early as 2005.

1961. As noted above, weapons caches seized from Special Groups by Coalition Forces in Iraq included many 107 mm artillery rockets with closely clustered DIO lot numbers and production dates between 2005 and 2007, as well as rounds and fuses for 60 mm and 81 mm mortars with DIO lot markings and 2006 production dates.

1962. In another example, in January 2006, police in the southern Iraqi city of Amara, near the Iranian border, captured seventy blocks of TNT explosives and seventy-nine blocks of plastic explosive, which were used by the Special Groups as components of IEDs, all with markings and lot numbers showing they were produced by DIO.

1963. In July 2010, the DOJ obtained a 27-count superseding indictment in *USA v. Mac Aviation et al.* charging the company and its officers with the following:

purchasing F-5 fighter aircraft parts, helicopter engines and other aircraft components from U.S. firms and illegally exporting them to Iran.... [...] Beginning as early as August 2005... through July 2008, the defendants solicited purchase orders from customers in Iran for U.S.- origin aircraft engines and parts and then sent requests for aircraft components to U.S. companies. These parts included helicopter engines, aircraft bolts and vanes, and canopy panels for the F-5 fighter aircraft. The defendants wired money to banks in the U.S. as payment for these parts and concealed from U.S. sellers the ultimate end-use and end-users of the purchased parts. The defendants caused these parts to be exported from the U.S. to third countries like Malaysia before causing them to be transshipped to Iran. [...] From 2005 [...] to 2006, the defendants caused canopy panels designed for the F-5 fighter aircraft, valued at approximately \$44,500, to be exported from the U.S. to Iran. The defendants falsely stated that the end user for the F-5 panels was the Republic of Nigeria. Instead, the panels were sold by the defendants to Sasadja Moavanate Bazargani, in Tehran, Iran for \$86,400. The purchase was arranged through the Iran Aircraft Manufacturing Industrial Company, known by its Iranian acronym as [IAMIC].

1964. According to the superseding indictment, Mac Aviation also shipped fifteen helicopter engines to IAMIC.

1965. These included ten Rolls-Royce Model 250 C-20B turboshaft engines, and five Rolls-Royce Model 250 C-20R2 turboshaft engines.

1966. Rolls-Royce Model 250 engines are used on IAMIC's 278 Shahed (military) helicopters (converted or adapted from the design of the American Bell 206B-III "Jet Ranger" and Bell 206L "Long Ranger" aircraft) flown by and developed for the IRGC.

1967. Between 2001 and 2005, SCB facilitated at least 21 LCs involving Mac Aviation for a total of close to \$8 million dollars.

1968. In each case, Mac Aviation was the nominal purchaser of the aircraft parts (Applicant), and the listed importer was either Iran Aircraft Industries, IHSRC, or IAMIC.

1969. Most, if not all of these LCs appear to have been financed, at least in part, by: Bank Saderat in London (IOVB) serving as the Reimbursing Bank; Bank Refah Iran serving as the Issuing Bank; SCB in London serving as the Advising Bank; SCB in Dubai serving as the Negotiating Bank; and SCB's New York branch serving as the Clearing Bank.

1970. Some of the transactions were financed through the CBI's Eurodollar credit line with SCB.

1971. The other transactions were financed through reimbursements in USD funds claimed by SCB, London primarily from Defendant Bank Saderat with funds deposited received into SCB London's USD account with SCB's New York branch for further credit to the Eurodollar account of Mac Aviation (SCB's customer).

1972. Notably, Bank Refah Iran was designated on February 17, 2011, by the U.S. Treasury Department for the following actions:

providing financial services to the Iranian Ministry of Defense and Armed Forces Logistics (MODAFL) and the Iran Aircraft Manufacturing Industrial Company [IAMIC]. In recent years, Bank Refah has facilitated millions of dollars of weapons-related purchases by MODAFL. These purchases included missiles and tanks and enabled Iran's leadership to maintain its fighter jets and submarines. Bank Refah also facilitated payments from [IAMIC] to businesses and individuals linked to Iran's weapons-related procurement.

1973. SCB's financing of MODAFL's clandestine and illegal acquisition of U.S. military (aircraft) spare parts did not fund or facilitate Iran's legitimate agencies, operations, or programs.

1974. Rather, SCB actively participated in a criminal conspiracy to help Iran's military and terror apparatus obtain critical machinery and equipment and aircraft spare parts it desperately needed to sustain its violent and unlawful activities.

1975. Monarch Aviation was an Iranian front company based in Singapore that was owned and controlled by husband and wife, Brian Douglas Woodford, a UK citizen, and Laura Wang-Woodford, a dual U.S. and UK citizen.

1976. It purported to be a manufacturer, dealer, and repairer of aircrafts and related parts. At least during the period between 2001 and 2007, SCB in Singapore maintained accounts for Monarch Aviation, Brian Douglas Woodford, and Laura Wang-Woodford.

1977. At least one Monarch Aviation account at the SCB-Singapore Battery Road branch was listed as account number ACU- 26-0-000106-3.

1978. Defendant Credit Suisse's Singapore Branch at 80 Raffles Place also maintained a USD account for Monarch Aviation with the account number K0100340.01.

1979. On January 15, 2003, Woodford and Wang-Woodford were indicted for, among other things, violations of the IEEPA, and U.S. export control laws.

1980. Laura Wang-Woodford was arrested on December 23, 2007, and later pled guilty to conspiring to violate the U.S. trade embargo by exporting U.S. origin aircraft components to Iran.

1981. According to the Superseding Indictment, between January 1998 and December 2007, Monarch Aviation, Jungda International Pte Ltd. (a Singapore based successor to Monarch Aviation), Brian Douglas Woodford and his wife, Laura Wang-Woodford, exported U.S. aircraft parts to Singapore and Malaysia, and then re-exported those items to companies in Tehran, Iran, without obtaining the required U.S. government licenses, while falsely listing their companies as the ultimate recipients of the parts on export documents filed with the U.S. government.

1982. Specifically, according to the Superseding Indictment and the U.S. Justice Department's Sentencing Recommendation, the funds transferred by Monarch Aviation paid for

Boeing CH-47 helicopter parts, including vane assemblies and bevel gears that were listed under category VIII on the United States Munitions List and illegally exported to Iran.

1983. The vane assemblies, part number 2-080-090-02 and national stock number (“NSN”) 44 2840-01-022-7142, and bevel gears, part number 2-080-013-03 and NSN 3020-00-860-7419, were manufactured by Honeywell International Inc., commercial and government entity (“CAGE”) 45 code 99193, in Phoenix, Arizona.

1984. These export-controlled, U.S. manufactured helicopter parts were used in Iran’s fleet of Boeing CH-47 heavy-lift utility helicopters that were refurbished by IAMIC.

1985. Iran’s CH-47 helicopters are operated by the Islamic Republic of Iran Army Aviation and the Islamic Republic of Iran Air Force.

1986. The Superseding Indictment also listed the following parts, *inter alia*, that were illegally exported to Iran by Monarch Aviation: o-rings, shear bolts, bushings, and rotary wing shields.

1987. The o-rings, identified by part numbers S6135-20059-102 (NSN 5331-01-270-1765) and S6135-20059-106 (NSN 5331-01-270-1766), were manufactured by Sikorsky Aircraft Corporation (CAGE code 78266) in Stamford, Connecticut.

1988. These export-controlled, U.S. manufactured parts were used in Iran’s fleet of Sikorsky SH-3D medium-lift utility/anti-submarine warfare helicopters that were refurbished by Iran IAMIC.

1989. Iran’s SH-3D helicopters are operated by the Islamic Republic of Iran Navy Aviation.

1990. The following parts were manufactured by Bell Helicopter Textron, Inc. (CAGE code 97499) in Fort Worth, Texas:

- a) Shear bolts, identified by part number NAS625-44 (NSN 5306-00-924-6261);
- b) Bushings, identified by part number 205-030-477-11 (NSN 1560-00-413-1492);  
and
- c) Rotary-wing shields, identified by part number 204-012-118-1 (NSN 1615-00-865-7914).

1991. These export-controlled, U.S. manufactured parts were used in the following Iranian rotary-wing aircraft:

- a) Bell AH-1J air-assault helicopters (refurbished by IAMIC);
- b) Bell UH-1 utility transport helicopters (refurbished by IAMIC);
- c) Iranian Helicopter Support and Renewal Company (“PAHNA”) 2091 air-assault helicopters (the PAHNA 2091 is an Iranian remanufactured version of the Bell AH-1J helicopter); and
- d) PAHNA 2-75 utility transport helicopters (the PAHNA 2-75 is an Iranian remanufactured version of the Bell UH-1 helicopter).

1992. Iran’s fleet of Bell AH-1J, Bell UH-1, PAHNA 2091 and PAHNA 2-75 helicopters are operated by the IRGC Air Force and Islamic Republic of Iran Army Aviation.

1993. From 1998 to 2005 (and likely thereafter), SCB facilitated at least 10 LCs financed by the CBI and Bank Refah with a total value of more than \$1.5 million dollars involving the shipment of U.S. origin aircraft parts sold by Monarch Aviation to MODAFL’s sub-agencies Iran Aircraft Industries, IHSRC, and IAMIC.

1994. Defendant Bank Saderat served as the Reimbursing Bank on most, if not all, of these transactions, which cleared through SCB’s New York branch on their way to Monarch Aviation’s accounts at SCB in Singapore.

1995. The aircraft parts were transported by Iran Air from Kuala Lumpur Airport, Malaysia, to Tehran Airport, Iran.

1996. SCB in Dubai served as the Negotiating Bank, and funds from the financing were paid to Monarch Aviation's account with SCB, Singapore through SCB Singapore's account with SCB, London, which in turn received the funds into its U.S. Dollar nostro account with SCB's New York branch from SCB – Bahrain's Offshore Booking Unit.

1997. In sum, various branches of SCB conspired with multiple MODAFL sub-agencies and Monarch Aviation, and used SCB's New York branch to both assist Iran's military in illegally acquiring contraband U.S. goods and to illegally disguise the illicit financing of those acquisitions through the SCB's New York accounts.

1998. SCB facilitated at least 316 additional transactions totaling \$12,110,565 in USD funds that involved Monarch Aviation at its accounts at SCB in Singapore. Dozens of those transactions post-date Woodford and Wang-Woodford's 2003 indictment.

1999. SCB's financing of MODAFL's clandestine and illegal acquisition of U.S. military spare parts through Monarch Aviation did not fund or facilitate Iran's legitimate agencies, operations, or programs. Rather, SCB actively participated in a criminal conspiracy to help Iran's military and terror apparatus obtain critical machinery and (aircraft) spare parts it desperately needed to sustain its violent and unlawful activities.

2000. Jetpower Industrial Ltd. was a Hong-Kong based Iranian front company purporting to be a trading company in aircraft parts controlled by Hok Shek Chan, a/k/a John Chan.

2001. In 2011, Chan was sentenced to 42 months for conspiring to illegally export, and attempting to illegally export, 10 indicators, used in C-130 military flight simulators, in violation of the Arms Export Control Act.

2002. According to the DOJ:

In 1993, Chan's company, Jetpower Industrial, was convicted in Hong Kong of export violations related to his export of U.S. military parts to Iran. Chan then changed his business practices to avoid detection. Rather than shipping U.S. origin goods directly from Hong Kong to Iran, Chan set up a sophisticated procurement network involving front companies and an experienced freight forwarder in Malaysia. Using his network, the defendant was engaged in the illegal procurement and export of aircraft parts from the U.S. for customers located in Iran, including several military related entities in Iran such as the Iranian Air Force, in direct violation of the U.S. Embargo against Iran since 1997.

2003. In fact, according to U.S. officials, Jetpower repeatedly and illicitly exported arms to Iran prior to Mr. Chan's arrest and conviction.

2004. At all relevant times, Jetpower was a customer of Bank Melli in Hong Kong.

2005. The full scope of SCB's involvement with and facilitation of Jetpower was extensive (involving at least dozens of transactions).

2006. Illegal payments totaling close to \$3 million dollars have specifically been identified, but the actual totals could be much higher.

2007. What is clear is that SCB repeatedly and knowingly facilitated the illegal shipment of U.S. origin aircraft parts sold by Jetpower to one of MODAFL's sub-agencies (IHSRC), and that Jetpower was a significant link in Iran's illegal weapons procurement chain.

2008. For example, in 2001-2002, Bank Refah (the Issuing Bank) issued a LC to MODAFL's sub-agency IHSRC that was to be reimbursed by Bank Saderat Plc (known then as Iran Overseas Investment Bank), then amended the LC to be available with SCB-Dubai.

2009. SCB's branches in New York, Singapore and Hong Kong were all instrumental in enabling Jetpower's receipt of payments at its Eurodollar account(s) with Bank Melli in Hong Kong.

2010. When Jetpower transported the contraband goods (U.S. helicopter parts) to MODAFL (using Iran Air), it asked Bank Melli in Hong Kong to present the documents required under the LC for payment to SCB Dubai.

2011. However, in many instances, SCB Dubai took at least four extra steps before Bank Melli in Hong Kong received the Eurodollar payment for Jetpower.

2012. Upon acceptance of the documents from Bank Melli, SCB Dubai used the CBI's Eurodollar credit facility with Standard Chartered Bank Dubai and sent instructions for a Eurodollar loan to be issued by SCB, Bahrain.

2013. SCB, Bahrain booked the loan and sent the proceeds in USD funds as payment under the LC through SCB's New York branch to National Westminster Bank's New York correspondent account for further credit to National Westminster, London for the Eurodollar account of its customer, Bank Melli, London.

2014. SCB, Dubai then sent instructions to Bank Melli, London to pay Bank Melli, Hong Kong upon receipt of USD funds.

2015. Variations on this process were undertaken on multiple LCs in USD funds for the benefit of MODAFL's sub-agency.

2016. In these cases, SCB, Bahrain knowingly cleared USD through SCB's New York branch for the illegal trade-finance transactions by repackaging the payments on the LCs as loans that secretly routed through the U.S. to Bank Melli Iran through various British banks.

2017. Jetpower, in most cases, ultimately received payment in USD funds to its Eurodollar bank account with Bank Melli Plc's branch in Hong Kong for these illicit transactions with IHSRC.

2018. According to BIS-Basel and the Hong Kong Monetary Authority, all USD transfers from SCB-Hong Kong to Jetpower's account with Bank Melli Plc's Hong Kong branch were cleared by the Hong Kong Clearing House Automated Transfer System, and settled by Defendant and co-conspirator HSBC's Hong Kong subsidiary.

2019. None of this illegal conduct was undertaken for any non-terroristic purpose for any agency, operation or program of Iran.

2020. The Iran Power Development Company, an Iranian government-controlled entity, has worked extensively for years with a network of Iranian companies known as the MAPNA Group.

2021. MAPNA International FZE is a UAE-based subsidiary. One of its directors, Mousa Refan, previously served as the first commander of the Air Force of the "Army of the Guardians of the Islamic Revolution [IRGC]."

2022. Another director, Afshin Rezaei, pled guilty in the U.S. District Court for the Northern District of Georgia on April 24, 2008, to the following:

one count of violating the IEEPA for the unlicensed export of computers to Iran via the United Arab Emirates. The computers were controlled for anti-terrorism reasons. On May 15, 2008, Rezaei was sentenced to six months of prison (credit for time served), followed by three years of supervised release, and agreed to forfeit \$50,000. On February 18, 2010, a 10-year denial of export privileges was imposed on Rezaei, pursuant to Section 11(h) of the EAA.

2023. During the Relevant Period, MAPNA International maintained a Eurodollar account with SCB, Dubai.

2024. Between 2001 and 2007, SCB facilitated at least 280 LCs involving MAPNA International FZE (as Beneficiary). In most cases, SCB, Dubai acted as the Advising Bank on these transactions.

2025. At least nine LCs involved SCB’s New York branch serving as the Clearing Bank for the transactions, and in some cases, SCB-London served as the Reimbursing Bank.

2026. SCB facilitated at least 7 LCs – totaling \$1,384,972 in USD funds – that involved the illegal shipment of U.S. origin goods to the Iran Power Development Company.

2027. The CBI served as the Issuing Bank on several of these LCs, and six of those seven involved goods shipped by IRISL.

2028. Of particular note, between 2003 and 2004, SCB knowingly facilitated at least four unlawful USD funds transfer transactions (cleared through its New York branch) that involved Eurodollar payments to Zener Electronics (UAE), a procurement company for Hezbollah.

2029. The Iran Power Development Company was listed as the Applicant for these transactions, and MAPNA was identified as the 1st Beneficiary, but assigned the payments under the Letters of Credit to Zener Electronics (UAE) as a “2nd Beneficiary.”

2030. Each unlawful trade-finance transaction involved U.S. goods.

2031. The CBI acted as the Issuing Bank on at least two of the transactions and SCB, Dubai acted as the Advising and Negotiating Bank.

2032. On at least one occasion, SCB-London served as the Reimbursing Bank for the payment to Zener Electronics, sending the credit through its New York branch to SCB Dubai’s account with SCB in New York.

2033. Upon receipt of the funds to its USD account with SCB in New York, SCB, Dubai instructed SCB’s New York branch to forward the funds to JP Morgan Chase in New York, which held an account for the Commercial Bank of Dubai.

2034. The Commercial Bank of Dubai, in turn, credited the account of its customer, Zener Electronics.

2035. These illicit transfers on behalf of MAPNA resulted in payments to Zener Electronics (a key link in Hezbollah's illicit supply chain) and were not for the non-terroristic benefit of any agency, operation, or program of Iran. In a Superseding Indictment filed in federal court on March 30, 2016, MAPNA was again implicated in the Conspiracy.

2036. This time, the DOJ charged multiple individuals with covert transactions in 2011 through a U.S. bank, wherein MAPNA's name was omitted from the transaction to hide its identity as a counterparty.

2037. The Iranian Helicopter Aviation Company, Ahwaz Pipe Mill Co. and Kala Naft56 are all subsidiaries of NIOC, which (as noted *supra*) was controlled by the IRGC during the Relevant Period.

2038. Between 1999 and 2001, SCB knowingly facilitated two illegal transactions totaling \$750,744 on behalf of the Iranian Helicopter Aviation Company (listed as the Applicant).

2039. The Beneficiary listed on both LCs was Limo Sarl. The goods involved in these transactions were U.S. origin helicopter parts.

2040. Payments for both transactions were cleared through SCB's New York branch, and refinanced under the CBI's Eurodollar credit facility with SCB, Dubai.

2041. The Paris-based Limo Sarl was directed by a Ms. Laleh Moein, reported to have also been in the employ of MOIS.

2042. Between 2002 and 2004, SCB knowingly facilitated four (4) illegal transactions totaling \$611,713 that involved U.S. origin goods illegally transported to Iran on behalf of Kala Naft.

2043. At least two of these transactions had SCB New York's branch serving as its Clearing Bank.

2044. As early as February 1998, Kala Naft was identified by the UK government "as having procured goods and/or technology for weapons of mass destruction programs."

2045. Kala Naft was also publicly identified as a NIOC subsidiary in a 2003 Commerce Department action that further stated that Kala Naft was a recipient of illegally exported U.S. origin oilfield equipment from the U.S.

2046. Between 2001 and 2006, SCB knowingly facilitated at least two illegal transactions totaling \$593,307 that involved U.S. origin goods illegally transported to Iran on behalf of Ahwaz Pipe Mill Co.

2047. The CBI was used as the Refinancing Bank, and SCB's New York branch served as the Clearing Bank.

2048. The listed beneficiary of the Ahwaz Pipe Mill Co. trade-finance transactions was a Cypriot company named Polygon Co. Ltd.

2049. Polygon's managing director and its owner had previously been indicted on November 19, 1992, in the Southern District of Florida for illegally conspiring to export oil field equipment and other goods, services and technology to Libya, demonstrating its history of illicit sanctions evasion on behalf of a State Sponsor of Terrorism.

2050. The litany of trade-finance and Eurodollar transactions discussed herein often involved counterparties (such as Mac Aviation, Jetpower and Polygon) with established track records of criminal activity on behalf of Iran.

2051. On June 20, 2005, SCB facilitated Khoram Sanat Producing Co.'s purchase of electromotors for hydraulic presses worth \$2.79 million dollars.

2052. The company is likely a subsidiary of another Iranian company known as "Alborz Steel."

2053. The nominal purchaser of the equipment was an Iranian front company in the UAE called Diamonds Steel.

2054. Diamonds Steel maintained one or more accounts with SCB, Dubai.

2055. Between 2001 and 2007, SCB, Dubai facilitated at least 173 transactions involving Diamonds Steel, totaling more than \$130 million.

2056. The aforementioned electromotors were illegally purchased from the United States with the LC facilitated by SCB's New York branch, which served as the Clearing Bank for the transaction, while SCB, Dubai served as the Advising Bank.

2057. SCB facilitated this transaction despite the fact the machinery required an export license because the equipment could be used for terrorist purposes.

2058. Specifically, hydraulic presses are the precise type of machinery required to manufacture EFPs.

2059. The production of an EFP shaped-charge munition requires at least a 10-ton hydraulic press in order to form sheets of copper and steel, respectively, into the necessary shaped-charge geometry for defeating the plating of American armored vehicles of the type used by the U.S. military in Iraq.

2060. Even assuming a steep mark-up in costs of delivery, SCB financed Iran's acquisition of approximately fifty (50) hydraulic presses capable of manufacturing more than a hundred EFPs per day.

2061. The hydraulic press machinery was transported to Iran by IRISL.

2062. Because LCs are intrinsically about the submission of detailed paperwork and required SCB (Credit Suisse and other Defendants) to examine and retain the documentation evidencing Iran's illegal procurement chain, SCB's knowledge of its role in the Conspiracy is indisputable.

2063. Furthermore, because Iran's illegal procurement chain was dependent on access to USD, SCB's (and other Defendants') participation in the Conspiracy was essential to its success.

2064. In sum, SCB was integral to Iran's inherently lethal and illegal conduct, which included a wide variety of money laundering techniques in the service of weapons procurement, arms shipments, acquisition of WMDs, and terror financing that substantially and foreseeably assisted MODAFL, the IRGC and Hezbollah in their campaign of violence and terror against Coalition Forces in Iraq.

2065. On August 6, 2012, the DFS issued an Order Pursuant to Banking Law § 39, which detailed SCB's legal and regulatory violations, its involvement in the conspiracy to provide of illegal banking services to Iran, which allowed terrorists to access the U.S. financial system.<sup>191</sup> That Order, among other things, stated as follows:

- a) "For almost ten years, SCB schemed with the Government of Iran and hid from regulators roughly 60,000 secret transactions, involving at least \$250 billion, and reaping SCB hundreds of millions of dollars in fees. SCB's actions left the U.S. financial system vulnerable to terrorists, weapons dealers, drug kingpins and

---

<sup>191</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Order entered by the New York Department of Financial Services on or about August 6, 2012, as if fully set forth herein.

corrupt regimes, and deprived law enforcement investigators of crucial information used to track all manner of criminal activity.”

- b) “In its evident zeal to make hundreds of millions of dollars at almost any cost, SCB undertook a course of conduct that included: falsifying business records; offering false instruments for filing; failing to maintain accurate books and records of all transactions effected and all actions taken on behalf of SCB; obstructing governmental administration; failing to report misconduct to the Department [of Financial Services] in a timely manner; evading Federal sanctions; and numerous other violations of law that, as with the above, have an impact upon the safety and soundness of SCB’s New York branch and the Department’s confidence in SCB’s character, credibility and fitness as a financial institution licensed to conduct business under the laws of this State [of New York].”
- c) “From January 2001 through 2007, SCB conspired with its Iranian Clients to route nearly 60,000 different USD payments through SCB’s New York branch after first stripping information from wire transfer messages used to identify sanctioned countries, individuals and entities . . . . . SCB intentionally withheld material information from New York and Federal regulators in its effort to service Iranian Clients.”

2066. The Order found that “SCB operated as a rogue institution” and that employees internally knew that its business dealings with Iran could subject U.S. and London management to “serious criminal liability.”

2067. Still, SCB willfully violated the law, as found by the DFS.

2068. Consistent with that distain of U.S. law, the DFS found that “SCB’s success in USD clearing for Iranian Clients stems from the documented willingness of its most senior management to deceive regulators and violate U.S. law. Worse yet, SCB apparently adopted this strategy with full knowledge of the risks involved.”

2069. The DFS Order shows these violations were continuous and substantial: with CBI/Markazi (an Iranian-owned sanctioned entity), SCB processed \$500 million in daily payments as the receipt bank for USD proceeds from daily oil sales made by the NIOC. SCB viewed the engagement as “very prestigious” because it was, in effect, acting as the treasurer to

the CBI. For Iranian U-Turn payments from 2005 and 2006 that SCB turned over to the DFS, SCB provided 2,626 transactions totaling over \$16 billion.

2070. After detailing SCB's egregious conduct, the DFS came to a damning conclusion:

Motivated by greed, SCB acted for at least ten years without any regard for the legal, reputational, and national security consequences of its flagrantly deceptive actions. Led by its most senior management, SCB designed and implemented an elaborate scheme by which to use its New York branch as a front for prohibited dealings with Iran – dealings that indisputably helped sustain a global threat to peace and stability. By definition, any banking institution that engages in such conduct is unsafe and unsound.

2071. In light of SCB's conduct, the DFS required SCB to show cause why the DFS should not revoke SCB's license to operate in the State of New York.

2072. On September 21, 2012, SCB and the DFS executed a Consent Order resolving charges that, from at least 2001 through 2007, SCB provided Eurodollar clearing and settlement services to Iranian customers subject to U.S. economic sanctions, with respect to approximately 59,000 transactions totaling approximately \$250 billion, through SCB's New York branch. DFS concluded that "SCB operated as a rogue institution."<sup>192</sup>

2073. On December 10, 2012, DOJ announced that SCB had agreed to forfeit \$227 million to the Justice Department for conspiring to violate the IEEPA, and the forfeiture was part of DPAs SCB entered into with Department of Justice and the Manhattan District Attorney's office for illegally moving millions of dollars through the U.S. financial system on behalf of, *inter alia*, sanctioned Iranian entities. SCB also entered into settlement agreements with OFAC and the Board of Governors of the Federal Reserve System, as well as with DFS.<sup>193</sup>

---

<sup>192</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order entered by the New York Department of Financial Services on or about September 21, 2012, as if fully set forth herein.

<sup>193</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference (1) the Settlement Agreement entered into between SCB and Department of Treasury on or about December 10, 2012, as if fully set

2074. DOJ filed a criminal information charging SCB with one count of knowingly and willfully conspiring to violate IEEPA. SCB waived the federal indictment, agreed to the filing of the information and, according to DOJ's press release, "accepted responsibility for its criminal conduct and that of its employees."

2075. DOJ's 2012 press release announcing the DPA quoted then-Assistant Attorney General Lanny Bruer as stating: "[f]or years, Standard Chartered Bank deliberately violated U.S. laws governing transactions involving Sudan, Iran, and other countries subject to U.S. sanctions. The United States expects a minimum standard of behavior from all financial institutions that enjoy the benefits of the U.S. financial system. Standard Chartered Bank's conduct was flagrant and unacceptable. Together with the Treasury Department and our state and local partners, we will continue our unrelenting efforts to hold accountable financial institutions that intentionally mislead regulators to do business with sanctioned countries."

2076. Manhattan District Attorney Cyrus Vance Jr. stated in the press release: "Investigations of financial institutions, businesses, and individuals who violate U.S. sanctions by misusing banks in New York are vitally important to national security and the integrity of our banking system. Banks occupy positions of trust. It is a bedrock principle they must deal honestly with their regulators. I will accept nothing less; too much is at stake for the people of New York and this country. These cases give teeth to sanctions enforcement, send a strong message about the need for transparency in international banking, and ultimately contribute to the fight against money laundering and terror financing."

---

forth herein; (2) the DPA entered into between SCB and Department of Justice on or about December 10, 2012, as if fully set forth herein; and (3) the Cease and Desist Order entered into between SCB and Board of Governors of the Federal Reserve System on or about December 10, 2012, as if fully set forth herein.

2077. Prior to entering into the 2012 DPA and its settlement with DFS, SCB retained Promontory Financial Group, LLC (“Promontory”) in 2009 to provide “consulting services in connection with the identification and collection of historical transaction records relating to cross-border financial transactions.”

2078. In the first half of 2010, SCB reported to various regulators, including the New York State Banking Department, DFS’s predecessor, that it had engaged in conduct related to the evasion of U.S. sanctions.

2079. On April 15, 2010, SCB hired Promontory again to identify, collect and review historical transaction records implicating sanctions violations.

2080. Thereafter, Promontory produced a number of reports and made various presentations to government authorities, including the New York State Banking Department (later DFS).

2081. These Promontory reports included, *inter alia*, interim reports throughout 2010, final reports in January and March of 2011, as well as updates to those final reports in October 2011.

2082. DFS relied in part upon the work conducted and presented by Promontory to identify the scope of SCB’s improper conduct prior to entering into the September 21, 2012 Consent Order.

2083. On June 18, 2013, Deloitte entered into a Settlement Agreement with DFS wherein it agreed, *inter alia*, to pay a penalty of \$10 million for misusing confidential information from other bank Defendants.

2084. For example, Deloitte provided SCB with copies of transaction review reports that Deloitte had prepared for these other clients and suggested to SCB management they be used as

templates for SCB's transactions review report, and agreeing to SCB's request that Deloitte remove a recommendation from its written final report explaining how "cover payment" messages used by SWIFT-NET (MT 202s) could be manipulated by banks to evade U.S. money laundering controls.

2085. On August 19, 2014, DFS announced an order regarding SCB's failures to remediate AML and combating the financing of terrorism compliance problems as required in SCB's 2012 settlement with DFS.

2086. Under the August 2014 DFS order, SCB was required to: (1) suspend dollar clearing through SCB's New York branch for high-risk retail business clients at SCB's Hong Kong subsidiary; (2) exit high-risk client relationships within certain business lines at SCB's branches in the UAE; (3) decline new dollar-clearing clients or accounts across its operations without prior approval from DFS; (4) pay a \$300 million penalty; and (5) take other remedial steps.<sup>194</sup>

2087. Additionally, according to an October 29, 2014 article in The New York Times, federal and Manhattan prosecutors have reopened their investigation into SCB.

2088. The New York Times reported that prosecutors were questioning whether SCB failed to disclose the extent of its wrongdoing to the government, thus imperiling SCB's 2012 settlement.

2089. In August 2015, DFS issued a "Report on Investigation of Promontory Financial Group, LLC."<sup>195</sup> The DFS report stated the following:

---

<sup>194</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Order entered by the New York Department of Financial Services on or about August 19, 2014, as if fully set forth herein.

<sup>195</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Report on Investigation of Promontory entered by the New York Department of Financial Services on or about August 18, 2015, as if fully set forth herein.

On April 15, 2010, Promontory was engaged by Standard Chartered's counsel to identify, collect and review historical transaction records "with certain countries or certain Specially Designated Nationals [] subject to sanctions" administered by OFAC. The engagement was known as Project Green.

As part of the engagement, Promontory produced a number of reports and made various presentations to the Bank and government authorities, including the New York State Banking Department. These reports included interim reports throughout 2010, final reports in January and March of 2011, and updates to those final reports in October 2011.

In connection with the Department's investigation of Standard Chartered, the Department relied in part upon the work conducted and presented by Promontory to identify the scope of the Bank's improper conduct and to determine an appropriate resolution of the investigation.

2090. DFS ultimately concluded that "There are numerous instances where Promontory, at the direction of the Bank or its counsel, or at its own initiative, made changes to 'soften' and 'tone down' the language used in its reports, avoid additional questions from regulators, omit red flag terms or otherwise make the reports more favorable to the Bank."

2091. Examples identified by DFS included a written communication on January 19, 2011, wherein "the Bank's counsel wrote to Promontory that the title of a particular slide entitled 'The 77 non-U-turn payments fell into 3 categories' – meaning the transactions were potential OFAC violations – should be made 'more bland' and suggested a rewording to 'Categories identified in Amendment Analysis.' Promontory made the change to the more vague language requested by the Bank."

2092. The DFS Report further found that "Promontory omitted certain timelines from the reports that would have indicated an increase in violations over time."

2093. The Report went on to cite a December 17, 2010 statement by a senior analyst at Promontory explaining:

Generally, the timelines serve a strong purpose with the Jersey payments. That is, there appears to be a positive trend over time to reduce the involvement with

potential violations. This will not be true with Dubai. I have a strong suspicion that people will not want to show the timelines for Dubai ([a particular client for which the Bank processed prohibited transactions] for example shows an upwardly sloping curve of violations). If we are going to go ahead with the visuals across the workstreams [*sic*], we should be cognizant of the graphics showing painful information and expect strong pushback from the bank and [the Bank's counsel].

2094. As described above, SCB's Dubai operations were a central hub for the IRGC's and MODAFL's illegal procurement efforts.

2095. In August 2015, The New York Times reported that SCB was once again under investigation: "The Justice Department is examining whether it committed sanctions violations beyond those covered in the 2012 deal, which centered on what the bank called 'Project Gazelle,' an effort to forge 'new relationships with Iranian companies.'"

2096. The Financial Times also reported in September 2015 the following:

Documents seen by the FT suggest that StanChart continued to seek new business from Iranian and Iran-connected companies after it had committed in 2007 to stop working with such clients. These activities include foreign exchange transactions that, people familiar with StanChart operations say, would have involved the US dollar....

The material reviewed by the FT depicts a bank — one of the few foreign lenders with a license [*sic*] to operate in the country — determined to keep working with Iranian companies. The status of numerous Iranian and Iran-connected entities was still being reviewed by StanChart as late as 2013, according to documents seen by the FT. These included entities that had internal "markers" and "blocks" placed against them, a way for the bank to flag up concern about links to Tehran. Many accounts belonging to Iranian or Iran-connected entities were indeed closed by 2007, as StanChart promised. But some, like Bank Saderat — which had sanctions imposed in 2006, or Bank Sepah — still had open accounts with no markers against them.

2097. Even as edited to be favorable to SCB, the 2011 Promontory Report provides a window into the vast array of wrongdoings undertaken by SCB in concert with Iran and its Agents and Proxies.

2098. As the Negotiating Bank on numerous illegal Iranian LCs, SCB received the detailed documentation for the shipment of goods, and knew that it was helping Iran's military and terrorist apparatus acquire prohibited U.S. goods and dual-use technologies.

2099. In sum, as the Negotiating Bank on numerous illegal Iranian transactions for Mahan Air and various MODAFL sub-agencies, and as an active conduit and money-launderer for the CBI and other sanctioned Iranian banks, SCB knew that: (1) it was dealing with Iran's military and terrorist apparatus; (2) it was conspiring to evade U.S. export sanctions; (3) it was laundering money in USD funds for Iran's military and terrorist apparatus; (4) its own customers were front companies for Iran's military and terrorist apparatus; (5) these customers were actively engaged in sanctions evasion and money laundering; and (6) that none of this illegal conduct was undertaken for the benefit of a legitimate agency, operation or program of Iran.

2100. SCB chose to use its presence in the United States to effectuate its crimes.

2101. By 2012, for nearly a decade, SCB programmatically engaged in deceptive and fraudulent misconduct in order to move at least \$250 billion through its New York branch on behalf of client Iranian financial institutions that were subject to U.S. economic sanctions, and then covered up its transgressions. These institutions included no less than the CBI, as well as Bank Saderat and Bank Melli, both of which are also Iranian State-owned institutions.

2102. In its evident zeal to make hundreds of millions of dollars at almost any cost, SCB undertook a course of conduct that included: (1) falsifying business records; (2) offering false instruments for filing; (3) failing to maintain accurate books and records of all transactions effected and all actions taken on behalf of SCB; (4) obstructing governmental administration; (5) evading Federal sanctions; and (6) numerous other violations of law that, as with the above, have an impact upon the safety and soundness of SCB's New York branch and the Department's

confidence in SCB's character, credibility and fitness as a financial institution licensed to conduct business under the laws of this State.

2103. From on or about January 26, 2001 and potentially continuing through the present, SCB conspired with Iran and its Agents and Proxies to route nearly 60,000 different USD payments through SCB's New York branch after first stripping information from wire transfer messages used to identify sanctioned countries, individuals and entities ("wire stripping").<sup>196</sup>

2104. All of this was done in violation of the prohibition against the "exportation ..., directly or indirectly, from the United States ... of any ... services to Iran or the Government of Iran."<sup>197</sup>

2105. Specifically, SCB ensured the anonymity of Iranian USD clearing activities through SCB's New York branch by falsifying SWIFT wire payment directions. When SCB employees determined that it was necessary to "repair" unadulterated payment directives,<sup>198</sup> they did so by stripping the message of unwanted data, replacing it with false entries or by returning the payment message to the Iranian Client for wire stripping and resubmission. Thus, SCB developed various ploys that were all designed to generate a new payment message for the New York branch that was devoid of any reference to Iran's Agents and Proxies.

---

<sup>196</sup> According to SCB's independent consultant, this figure represents about 30,000 messages that were sent to SCB's New York branch by SCB's London office, mainly on behalf of state-owned Iranian banks, and approximately 30,000 messages from SCB's branch in Dubai, United Arab Emirates, to SCB's New York branch on behalf of Iranian-owned banks, corporations and other unknown entities.

<sup>197</sup> 31 C.F.R. § 560.204.

<sup>198</sup> Under SCB's "repair procedure" overseas employees screened payment messages – before they were communicated to its New York branch – in order to ascertain if any messages contained information that identified Iranian Clients.

2106. Despite this extensive history of illegal conduct, SCB's chairman claimed in early 2013 that its illegal conduct were "clerical errors" and not "willful acts:" "We had no willful act to avoid sanctions; you know, mistakes are made – clerical errors – and we talked about last year a number of transactions which clearly were clerical errors or mistakes that were made."<sup>199</sup> The U.S. government took the unusual step of forcing SCB to apologize for those statements and issue an accurate statement about SCB's purposeful, illegal conduct.<sup>200</sup>

2107. After the U.S. government required SCB to accept responsibility and be truthful, SCB's chairman stated the following in the statement:

My statement that SCB "had no willful act to avoid sanctions" was wrong, and directly contradicts SCB's acceptance of responsibility in the deferred prosecution agreement and accompanying factual statement.

Standard Chartered Bank, together with me, Mr. Peter Sands and Mr. Richard Meddings, who jointly hosted the press conference, retract the comment I made as both legally and factually incorrect. To be clear, Standard Chartered Bank unequivocally acknowledges and accepts responsibility, on behalf of the Bank and its employees, for past knowing and willful criminal conduct in violating US economic sanctions laws and regulations, and related New York criminal laws, as set out in the deferred prosecution agreement. I, Mr. Sands, Mr. Meddings, and Standard Chartered Bank apologize for the statements I made to the contrary.<sup>201</sup>

2108. Thus, even after avoiding criminal prosecution for its illegal conduct, SCB—only months after entering into the deferred prosecution agreements—continued to refuse to accept responsibility for its violations of U.S. sanctions and participation in the Conspiracy.

2109. The criminal conduct of SCB is representative of the criminal conduct exhibited by the other defendant banks. Each made millions moving billions for Iran.

---

<sup>199</sup> *US Regulators force Standard Chartered to retract Iran sanctions comments*, The Guardian (March 21, 2013), available at <https://www.theguardian.com/business/2013/mar/21/standard-chartered-us-regulators-iran-sanctions>.

<sup>200</sup> *Id.*

<sup>201</sup> Standard Charter PLC, *Statement by Sir John Pearce, Chairman* (Mar. 21, 2013), [https://www.sc.com/hk/investor-relations/\\_documents/en/news/20130321.pdf](https://www.sc.com/hk/investor-relations/_documents/en/news/20130321.pdf).

2110. SCB, as all Defendants, were in a position where they could disguise such wire transfers. This was made possible by the fact almost all of the laws enacted and tools developed, put the responsibility to detect such wire transfers squarely on the shoulders of the large banks that process such wire transfers.

#### **8. RBS' Participation in the Conspiracy**

2111. RBS agreed to, and participated in, the Conspiracy.

2112. Beginning by at least the mid-1990s and continuing through at least 2009, RBS had a continuous, ongoing relationship with Iran and its Agents and Proxies.

2113. From at least 2002 to 2011, RBS conducted more than 3,500 transactions valued at approximately \$523 million through New York correspondent banks involving sanctioned entities, including Iran and Iranian sanctioned entities.

2114. Moreover, these transfers not only overlapped with the Terrorist Attacks that killed, maimed, or otherwise injured Plaintiffs and Plaintiffs' family members, but also occurred at a time when RBS knew that funds it transferred on behalf of Iran and its Agents and Proxies, were being used to support the Terrorist Groups responsible for the Terrorist Attacks that injured or killed Plaintiffs.

2115. In May 1995, top officials of RBS in Amsterdam e-mailed the entire management in Europe, Asia, South America, Africa, the Caribbean, and North America, advising them that any financial transactions in USD funds undertaken for or on behalf of Iranian persons or banks were subject to seizure or blocking in the United States.

2116. Soon after President Clinton signed the Executive Order implementing sanctions against Iran in May 1995, Iranian banks sought the services of RBS and other banks in aiding Iran to circumvent U.S. laws.

2117. RBS employees were aware of these requests, discussed these requests with the other co-conspirator banks, and thereafter approved of RBS conducting the illegal transactions, contrary to the advice of its outside counsel that RBS's involvement in such transactions would potentially violate U.S. law.

2118. From approximately 1995 until at least 2011, RBS conspired with the Iranian Bank co-conspirators (including the CBI, Bank Melli Iran, and Defendant Bank Saderat) and their agents to conceal evidence of RBS's financial transactions from the U.S. government, law enforcement, and intelligence agencies, as well as U.S. financial institutions charged with detecting and blocking certain Iranian transactions.

2119. RBS was, at the same time, aware that numerous other non-Iranian financial institutions were engaged in the Conspiracy to conceal evidence of the Iranian Bank co-conspirators' financial transactions from the U.S. government, law enforcement and intelligence agencies, as well as U.S. financial institutions charged with detecting and blocking certain Iranian transactions.

2120. From approximately 1995 until in or about 2005, RBS furthered the Conspiracy by methodically removing and/or falsifying payment messages on its funds transfer systems to disguise the movement of hundreds of millions of USD illegally through the U.S. financial system on behalf of the Iranian Bank co-conspirators (including Bank Melli Iran).

2121. In furtherance of the Conspiracy, RBS and the Iranian Bank co-conspirators developed methods by which RBS would format USD payments so that such payments would evade U.S. sanctions and detection by automated filters used by financial institutions in the United States.

2122. When RBS employees received payment messages from the Iranian Bank co-conspirators that contained certain words that could trigger a U.S. bank's automated OFAC filter software algorithms, RBS would manually alter or amend the messages (i.e. "strip" the transactions) to ensure the transaction would go undetected when it was cleared and settled by financial institutions in the United States.

2123. RBS thereby caused financial institutions in the United States to process transactions involving the Iranian Bank co-conspirators that U.S. financial institutions would not otherwise have processed.

2124. Like SCB and the other Defendants, certain offices, branches, and subsidiaries of RBS also altered LCs and foreign exchange transactions involving USD funds by replacing the names of the Iranian Bank co-conspirators (including Bank Melli Iran) on those transactions.

2125. Beginning as early as 1995 and continuing until in or about 2005, RBS undertook various acts in furtherance of the Conspiracy. For example: The Dubai branch of RBS created procedures and guidelines to facilitate the processing of prohibited USD transactions.

2126. For instance, one section of the RBS payment manual entitled "Special Conditions" listed specific instructions on how to effectuate these payments and avoid OFAC filters.

2127. A specific instruction from this manual stated: "Payments by order of Iranian Banks ...maintaining accounts with ABN [RBS], Dubai are to be handled with extra care to ensure the wordings "Iran" etc. are not mentioned in the payment due to OFAC regulations."

2128. In June 1995, an Iranian Bank co-conspirator requested RBS officials in Dubai that RBS act as a conduit for all USD transactions for that Iranian bank in Dubai.

2129. The Iranian bank requested that all of its USD funds transfer be routed through, or be issued in the name of, RBS and carry no reference to the fact these payments were issued on its behalf, and that all of its USD receipts would come into RBS's account.

2130. Thereafter, RBS undertook various specific acts to conceal its actions on Iran's behalf.

2131. RBS instructed the Iranian Bank co-conspirators to include the code word "SPARE" in their payment messages through the bank so that RBS could first segregate these messages from normal message payment processing, and then amend the message by removing/altering any potentially problematic text, i.e. any reference to Iran.

2132. The payment message would then be stopped by RBS, routed into a special queue, and manually altered to avoid being blocked by any OFAC sanctions screening filters.

2133. In this manner, RBS assisted sanctioned entities, and ensured the processing of transactions by formatting payment order messages so they would not be rejected or blocked by OFAC filters at financial institutions in the United States.

2134. RBS added to its payment manuals the "Special Conditions" that were to be used on behalf of the Iranian Bank co-conspirators in order to evade detection and circumvent the laws of the United States.

2135. RBS used these same or materially similar procedures with respect to LCs in USD funds, and the processing of USD-denominated checks and traveler's checks.

2136. RBS and the Iranian Bank co-conspirators knew and discussed the fact without such alterations, amendments, and code words, the automated OFAC filters at clearing banks in the United States would likely halt most of the payment messages and other transactions, and, in

many cases, would reject or block the sanctions-related transactions and report the same to OFAC.

2137. In order to circumvent U.S. sanctions, certain Iranian Bank co-conspirators requested that RBS omit their names and BICs from payment order messages sent by RBS to its U.S. correspondent banks. RBS complied with the requests of these Iranian Bank co-conspirators, and omitted their names and identifiers in order to help bypass OFAC filtering mechanisms of U.S. financial institutions.

2138. RBS also used SWIFT-NET MT 202 cover payment messages to shield the identities of the Iranian Bank co-conspirators.

2139. Instead of using serial MT 103 payment messages that require the names and details of counter-parties to transactions, RBS began using MT 202 cover payment messages expressly for the purpose of avoiding revealing the true identity of the ordering customer and beneficiary party for USD payments sent through financial institutions in the United States.

2140. The CBI coordinated with RBS's Central Bank Desk in Amsterdam regarding the procedure to be followed for repayment of USD deposits to their accounts with European Banks in London.

2141. This procedure stipulated that payment order messages sent to U.S. clearing banks for payment of USD funds to the CBI should not contain any reference to the Central Bank of Iran or any other reference relating to Iran.

2142. In or about June and July 1995, officials at RBS's Amsterdam Headquarters and New York offices were advised by counsel that the proposal by Iranian banks for RBS to serve as a conduit or means to bypass and avoid U.S. sanctions against Iran risked breaching U.S. law.

2143. An internal memorandum generated by RBS at the time stated the proposed fund transfer mechanics“are an attempt to circumvent the Iranian trade embargo. Given that violations of the Executive Order and OFAC regulations carry substantial penalties, not to mention the negative publicity,” the proposal must be “strictly scrutinized and ABN Amro [RBS] must weigh the risks before proceeding with any such transfers.”

2144. Also, in June 1995, another Iranian Bank co-conspirator sent a written communication to certain banks in the UAE and the Iranian Bank’s correspondent banks instructing those banks to undertake USD funds transfers for the Iranian bank in the name of a European financial institution “WITHOUT MENTIONING OUR BANK’S NAME” to defeat and circumvent the sanctions imposed upon Iran by the United States.

2145. Like the first request, the Iranian Bank co-conspirator’s request was forwarded to officials located in several departments of the Amsterdam Headquarters of RBS.

2146. As early as 1997, in an internal strategy paper for the Middle East and Africa region named “Desert Spring,” prepared by RBS’s Middle East and Africa Regional Office, RBS described a “product initiative” with “opportunities in LC discounting for Central Bank and Bank Melli, Iran” and “deposit mobilization from Iranian nationals.”

2147. On or about February 5, 2000, an official at the Dubai branch of RBS wrote to a Regional Director of one of the Iranian Bank co-conspirators assuring him that RBS would take care of carrying out the scheme to evade and defeat the U.S. sanctions.

2148. The RBS official’s note stated: “[w]e understand the special nature of your US\$ transactions and will ensure that all operations departments concerned are properly briefed regarding this, as well.”

2149. A July 19, 2003 e-mail written by John Ciccarone, Head of USD Payments Product Management at RBS's New York branch, discussed the use of MT 202 cover payments, stating: "There is no way the payment will get stopped as all NY ever sees is a bank to bank instruction."

2150. In a July 25, 2003 e-mail, John Philbin, Senior Relationship Banker for Iranian Banks, wrote to Ciccarone:

Surely Iran is the most obvious case in point for these structures. Twenty four years of US sanctions and OFAC listing and Iran continues to sell oil and gas in USD. And, it imports and pays in USD as well. All of this is clearly done through accounts in Europe and elsewhere. There is a very good case to be made for getting an overall acceptance that when issues are purely US, we should not be a part of it. In fact, we should see it as an opportunity. OFAC is not the Bible for money laundering (e.g. Cuba is prominent on OFAC). It is a tool of broader US policy. We therefore need to distinguish between US foreign policy on the one hand and AML/anti-Terrorism on the other, however much the US administration may wish to insist that the two are closely linked. It is well worth working on a solution for clients who find themselves in this position or who fear (Syria, Saudi Arabia) that they, one day soon might find themselves there.

2151. Also in 2003, Diane Perrin, a member of RBS's Group Compliance team at Defendants' Amsterdam Head Office, stated that "as a European Institution, we do not comply with US Sanctions because those sanctions are politically motivated."

2152. A 2003 memorandum entitled "Proposal for Establishing a Representative Office in Tehran, Iran" drafted by RBS's Country Representative in the UAE, Jan Willem van den Bosch, similarly stated:

The Central Bank of Iran is faced with difficulties for USD-denominated clearing transactions due to sanctions imposed by the US. OFAC filter impounds all Iran related payments and receipts in the US. The Swiss and other European Banks have worked out a solution for this. The payment instructions are sent directly to the beneficiary's bank and cover payment is made to the beneficiary bank's US Correspondent as inter-bank payments.

2153. Bosch later coordinated the meeting in Dubai between RBS's Managing Board Member and CFO Tom De Swann and top functionaries of the CBI, including Aziz Farrashi, CBI's Director General.

2154. During the meeting with the CBI's officials, RBS officials discussed the establishment of the Representative Office by RBS in Tehran and further business development, including the acceptance of USD deposits by the CBI's Desk in Amsterdam.

2155. In an April 20, 2004 e-mail, the aforementioned Philbin mentioned the possibility of using a Jersey Special Purpose Vehicle as a way to circumvent OFAC restrictions:

Mike Louwerens [RBS's Vice President and Senior Analyst of Country Risk Management Department] mentioned this to me today and sent the attached. The structure below is very interesting and could have applicability for the banks in Iran as well. But whether that is the case or not, what is clear is that this structure envisages our making and receiving payments in USD which will clear through AA *in New York*. And for which Mike Bowman sees no objection. I am sending a second note in which OEM (Maarten Seckel) gives a go ahead based on Bowman's nihil obstat. The Way for our doing significant business with the Iranian banks in cash may yet be clear.

(Emphasis added).

2156. On December 19, 2005, RBS and its New York branch entered into a Written Agreement with the Federal Reserve Banks of New York and Chicago and other regulators that had detected deficiencies at RBS's New York Branch relating to AML policies, procedures, and practices that included:

a pattern of previously undisclosed unsafe and unsound practices warranting further enforcement action.... A. ABN AMRO [RBS] lacked adequate risk management and legal review policies and procedures to ensure compliance with applicable U.S. law, and failed to adhere to those policies and procedures that it did have. As a result, one of ABN AMRO's [RBS's] overseas branches was able to develop and implement "special procedures" for certain funds transfers, check clearing operations, and letter of credit transactions that were designed and used to circumvent the compliance systems established by the Branches to ensure compliance with the laws of the U.S. In particular, the "special procedures"

circumvented the Branches' systems for ensuring compliance with the regulations issued by the [OFAC] (31 C.F.R. Chapter V).

2157. U.S. regulators also found that “[p]rior to August 1, 2004, the New York Branch processed wire transfers originated by Bank Melli Iran, a financial institution owned or controlled by the Government of Iran. The payment instructions on the wire transfers had been modified by one of ABN Amro's [RBS's] overseas branches such that any reference to Bank Melli Iran was removed.”

2158. U.S. regulators also found that “[p]rior to August 1, 2004, the Branches advised a number of letters of credit issued by Bank Melli Iran. The letters of credit had been reissued by one of ABN Amro's [RBS's] overseas branches such that any reference to Bank Melli Iran was removed.”

2159. As DOJ later concluded: “Each year between and including 1996 and 2004, ABN [RBS] caused ABN's [RBS's] U.S. affiliate to file false, misleading, and inaccurate Annual Reports of Blocked Property to OFAC. In each of those reports, the U.S. affiliate of ABN [RBS] certified to OFAC that all information provided was accurate and that all material facts in connection with the report had been set forth.”

2160. Nonetheless, in September 2004, Michael Louwerens, RBS's Vice President and Senior Analyst of Country Risk Management Department, traveled to Iran at the behest of RBS's Head Office and reported back that he had communicated with the Chief Representative of Defendant and co-conspirator HSBC in Tehran (presumably John Richards) and concluded that RBS's payment procedures (to conceal Iranian financial activity) were in line with prevailing market practices of HSBC and other banks.

2161. In addition, RBS's then-New York branch was the conduit for at least 90 post-U.S. designation transactions on behalf of IRISL and its various front companies through March 2010.

2162. On May 10, 2010, DOJ issued a press release announcing that ABN Amro's successor entity, Defendants Royal Bank of Scotland N.V., had agreed to forfeit \$500 million to the United States in connection with a conspiracy to defraud the United States, to violate the IEEPA, the Trading with the Enemy Act, and the BSA.

2163. In connection with a DPA RBS entered into, a criminal information was filed in the U.S. District Court for the District of Columbia charging Defendants with one count of violating the BSA, and one count of conspiracy to defraud the United States and violate the IEEPA and the Trading with the Enemy Act. RBS waived indictment, agreed to the filing of the information, and, according to the press release "accepted and acknowledged responsibility for its conduct."

2164. According to the criminal information, RBS's participation in the conspiracy continued "until in or about December 2007." Prior to that time, RBS willfully and knowingly conspired, *inter alia*, to "engage in financial transactions with entities affiliated with Iran ... in violation of the IEEPA, Title 50, United States Code, Section 1705, and regulations and embargoes issued thereunder...."

2165. The criminal information confirmed that RBS was an active participant in the Conspiracy, including the following statements:

- a) "It was part of the conspiracy that the defendant discussed with the co-conspirators how to format United States Dollar message payments so that such payments would avoid detection by automated filters used by financial institutions in the United States and thus evade United States sanctions."

- b) "It was part of the conspiracy that the defendant removed names and references to the co-conspirators in United States Dollar message payments routed through the United States."
- c) "It was part of the conspiracy that the defendant altered the names and references to the co-conspirators in United States Dollar message payments routed through the United States."
- d) "It was part of the conspiracy that the defendant instructed the co-conspirators to use code words in United States Dollar payment messages."
- e) "It was part of the conspiracy that the defendant created a special processing queue to manually and materially alter any of the co-conspirators' United States Dollar message payments that were to be routed through the United States."
- f) "It was part of the conspiracy that the defendant created "Special Conditions" in the defendant's payment manuals in order to process any co-conspirators' United States Dollar transactions."
- g) "It was part of the conspiracy that the defendant caused its United States affiliates to submit materially false and misleading reports or statements to the United States Department of the Treasury, OFAC."

2166. The Factual Statement in the May 10, 2010 DPA with RBS also confirmed that ABN (which RBS subsequently acquired) was part of the Conspiracy:

- a) "Beginning after the announcement of U.S. sanctions against countries and entities designated as supporting international terrorism in the mid-1990s, certain offices, branches, subsidiaries, and affiliates of ABN systematically violated the laws of the United States by conspiring with entities subject to U.S. sanctions on ways to circumvent the sanctions and by facilitating the movement of hundreds of millions of dollars illegally through the U.S. financial system on behalf of those sanctioned entities."
- b) "ABN engaged in this criminal conduct by: (a) methodically removing or falsifying references from outgoing United States Dollar ("USD") payment messages that principally involved countries such as Iran, Libya, the Sudan, and Cuba, banks from Iran, Libya, the Sudan or Cuba, or persons listed as parties or jurisdictions sanctioned by the [OFAC] (collectively, the "Sanctioned Entities"); (b) advising the Sanctioned Entities how to evade automated filters at financial institutions in the United States; and (c) willfully failing to maintain or establish appropriate Bank Secrecy Act ("BSA") and Anti-Money Laundering ("AML") procedures or to conduct effective due diligence reviews concerning foreign correspondent accounts."

- c) “Additionally, as part of this criminal conduct, ABN: (a) caused financial institutions in the United States to process transactions involving Sanctioned Entities, including banks from Iran, Libya, the Sudan, and Cuba, that the U.S. financial institutions would not otherwise have processed; and (b) prevented financial institutions in the United States from filing required BSA and OFAC-related reports with U.S. authorities.”
- d) “Certain offices, branches, and subsidiaries of ABN used procedures to alter USD payment messages by: (a) removing names and references to Sanctioned Entities from payment messages; (b) altering the names of the Sanctioned Entities; (c) instructing the Sanctioned Entities to include the code word “SPARE” in their payment messages so ABN could first segregate these messages from normal message payment processing and then amend the message by removing/altering any potentially problematic text; (d) creating a manual queue to ensure certain payment methods and language were used to effectuate the sanctioned payments; (e) replacing the names of Sanctioned Entities with ABN on letters of credit and foreign exchange transactions; and (f) adding to payment manuals the “Special Conditions” that were to be used for certain Sanctioned Entities in order to circumvent the laws of the United States. In addition, ABN used these same procedures for Sanctioned Entities with respect to letters of credit, and the processing of USD checks and traveler’s checks. ABN and the Sanctioned Entities knew and discussed the fact without such alterations, amendments, and code words, the automated OFAC filters at clearing banks in the United States would likely halt the payment messages and other transactions, and, in many cases, would reject or block the sanctions-related transactions and report the same to OFAC. ABN knew that financial institutions in the United States could choose not to process permissible payments on behalf of any of the Sanctioned Entities. By making the transactions appear to be on behalf of ABN and not the Sanctioned Entities, ABN’s actions effectively denied the financial institutions in the United States that opportunity. ABN therefore also prevented the financial institutions in the United States from filing required BSA and OFAC-related reports with the U.S. authorities. Further, because of ABN’s actions, civil monetary judgments against the Sanctioned Entities could not be enforced in the United States, nor could the Sanctioned Entities’ funds be seized since no one, other than ABN, knew the money actually was owned by the Sanctioned Entities. ABN management identified these practices in 2004 and terminated them in 2005. The implementation of more robust controls continued through 2006.”
- e) “In addition to altering USD payment messages, ABN conspired with the Sanctioned Entities about how to format USD payments so that such payments would evade U.S. sanctions and detection by automated filters used by financial institutions in the United States. When ABN employees received payment messages from the Sanctioned Entities that contained words that could trigger a U.S. bank’s OFAC filter, ABN would manually alter or amend the messages to ensure that they would not be detected by financial institutions in the United

States. ABN's actions in facilitating these payments were motivated by the profit ABN could make from the Sanctioned Entities."

f) "Each year between and including 1996 and 2004, ABN caused ABN's U.S. affiliate to file false, misleading, and inaccurate Annual Reports of Blocked Property to OFAC. In each of those reports, the U.S. affiliate of ABN certified to OFAC that all information provided was accurate and that all material facts in connection with the report had been set forth."<sup>202</sup>

2167. The Factual Statement Section further details ABN's conduct in evading U.S. sanctions on Iran and other Sanctioned Entities, including ABN's knowledge that Iran was subject to sanctions as a State Sponsor of Terrorism: "ABN's management, lawyers, auditors, and compliance officials were well aware of U.S. sanctions against Sanctioned Entities. For instance, on or about May 18, 1995, top officials of ABN in Amsterdam sent an electronic mail message to the entire management of ABN in Europe, Asia, South America, Africa, the Caribbean, and North America, advising and noting that any financial transactions in USD undertaken for or on behalf of Iranian persons or banks were subject to seizure or blocking in the United States."

**URGENT**

**US Sanctions against Iran**

Your attention is urgently drawn to the unilateral imposition of sanctions by the USA against Iran. Whilst no clear picture of the exact extent of the sanctions has yet emerged, all offices should give special attention to any payment traffic in US\$ in favour of Iranian beneficiaries of any sort; it is known that such US\$ transfers are being blocked in the USA.

2168. On October 12, 2013, RBS settled with OFAC after violating U.S. law in furtherance of the Conspiracy detailed herein. The OFAC settlement also recites how RBS participated in the Conspiracy, including:

---

<sup>202</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPA entered into with the DOJ on or about May 10, 2010, as if fully set forth herein.

- a) "In 1997, National Westminster Bank ("NatWest") - which RBS acquired in March 2000 - began acting as a correspondent bank for Bank Melli Iran ("Bank Melli") and its wholly-owned UK subsidiary, Melli Bank Plc ("Melli Plc"). As part of its operations in serving as a correspondent bank, RBS processed U.S. Dollar ("USD") transactions for and on behalf of Bank Melli and Melli Plc and these banks' customers. NatWest (and later RBS) conducted USD payments for the Iranian banks by sending Society for Worldwide Interbank Financial Telecommunication ("SWIFT") MT103 payment messages directly to non-U.S. beneficiary banks, and SWIFT MT202 payment messages (or "cover payments") to U.S. clearing banks. Although the payment messages sent to non-U.S. beneficiary banks included complete payment information, including the names of the Iranian banks and customers, the payment instructions sent to U.S. financial institutions did not include any references to the Iranian parties."
- b) "Beginning in late 2002, several employees within RBS responsible for managing and/or overseeing certain global correspondent banking relationships - including the SRM – ME and a Senior Manager - Trade, with copies to the Head of Credit Risk for Correspondent Banking - worked with two Senior Project Analysts in Change Management, Payment Operations who were involved in the implementation of the ProPay system, in order to manipulate outbound payment messages involving Iran. Over the next several months, the group developed a procedure within ProPay that would allow RBS to send USD payments to Iran and/or Iranian banks through a third-country bank that would omit information about the Iranian nexus in any cover payments sent to U.S. financial institutions. According to this procedure, RBS payment operators would list the actual name of the Iranian bank - rather than the Iranian bank's Bank Identifier Code ("BIC") - in the beneficiary bank field of the payment instructions with a country code of Great Britain rather than Iran. This method allowed the non-U.S. bank to identify the ultimate Iranian beneficiary bank for the payment from the information contained in the MT103. The manner in which this information was styled, however, prevented the bank's payment system from automatically including references to the Iranian bank or Iran in related cover messages and resulted in the data being omitted from instructions sent to U.S. clearing banks."<sup>203</sup>

2169. As part of this process, RBS instructed its employees to omit information from USD transactions that would inform banks in the United States the transaction violated U.S. sanctions:

**IMPORTANT: FOR ALL US DOLLAR PAYMENTS TO A COUNTRY SUBJECT TO US SANCTIONS, A PAYMENT MESSAGE CANNOT**

---

<sup>203</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Settlement Agreement with the Department of Treasury entered into on or about October 12, 2013, as if fully set forth herein.

CONTAIN ANY OF THE FOLLOWING: 1. The sanctioned country name. 2. Any name designated on the [OFAC] restricted list, which can encompass a bank name, remitter or beneficiary.

2170. RBS intentionally processed these illegal transactions in such a manner as to avoid detection by United States regulators and law enforcement. In particular, RBS removed identifying information about Iran and Iranian entities from the SWIFT payment messages, used non-transparent cover payment methods that were stripped of important identifying information about the underlying party, and instructed Iranian clients to include notes or code words in requested payment transactions that would trigger “special processing” by RBS employees to ensure RBS employees would hide identifying information to avoid having the payment requests picked up by RBS personnel and OFAC filter software.

2171. As a result of this conduct, RBS failed to maintain, and caused other banks to fail to maintain, adequate and correct financial records of USD payment transactions and the omitted and modified payment requests set forth above likewise prevented RBS and other banks from maintaining adequate and complete financial records as required by state and federal law.

2172. Based on the conduct described above, RBS entered into Consent Order with the DFS on RBS’s violation of New York and U.S. law.<sup>204</sup>

2173. Further, the Federal Reserve Board issued a Consent Order to cease and desist and a civil money penalty assessment of \$50 million against RBS Group and RBS Plc for lacking adequate risk management and legal review policies and procedures to ensure that activities conducted at offices outside the United States comply with applicable OFAC Regulations, and

---

<sup>204</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order, as if fully set forth herein.

for allowing certain of its business lines to implement policies and procedures for processing transactions that violated the law.<sup>205</sup>

2174. In conjunction with reaching these agreements, RBS agreed the following facts are true and correct:

- a) From at least 2002 to 2011, in order to allow its Iranian customers and beneficiaries to gain access to the U.S. financial system and to US dollars with anonymity, RBS established and implemented a systematic procedure for processing USD payments whereby information that could be used to identify sanctioned parties to a given transaction would be omitted from payment messages sent to correspondent banks in New York.
- b) RBS provided its employees written instructions containing step-by-step guidelines on how to create and route USD payment messages involving sanctioned entities like Iran through the United States to avoid detection. These instructions included the following:

IMPORTANT: FOR ALL US DOLLAR PAYMENTS TO A COUNTRY SUBJECT TO US SANCTIONS, A PAYMENT MESSAGE CANNOT CONTAIN ANY OF THE FOLLOWING:

1. The sanctioned country name. 2. Any name designated on the Office of Foreign Asset Control (OFAC) restricted list, which can encompass a bank name, remitter or beneficiary ...

- c) In fact, RBS went so far as to include these instructions in RBS's Business Support Manual, made the instructions available to its relevant employees, posted these instructions on RBS's Intranet, and disseminated these instructions to RBS's International Banking Center payment processors;
- d) This illegal payment processing was knowingly supported by senior RBS employees, including RBS's Group Head of AML, as well as the Head of Operational Risk, Global Transaction Services, and the Head of Global Banking Services for Europe, Middle East and Africa, who were fully aware of, and in some instances even provided, the Iranian USD transaction instructions to RBS employees. For example, on at least one occasion, the Head of Operational Risk warned all Payment Processing Center Heads via email to: "Please take care when making [payments] ... to ensure that there is no wording within the message that could potentially lead to the payment being stopped e.g. reference to a sanctioned country ..."

---

<sup>205</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order, as if fully set forth herein.

- e) Moreover, even after RBS adopted official bank policies in July 2006 to curb the illegal transaction processing, RBS nevertheless continued to process transactions through New York in a non-transparent manner using these and other means.

2175. Based on this and other illegal conduct on behalf of Iran aimed at the United States financial system, RBS chose to enter into a sweeping Consent Order, admitting that its conduct was at odds with U.S. national security and foreign policy and raised serious safety and soundness concerns for regulators, including the obstruction of governmental administration, failure to report crimes and misconduct, offering false instruments for filing, and falsifying business records and violated New York State banking laws, including Penal Law §§ 175.10, 175.35, 195.05 and 3 N.Y.C.R.R. 300.1.<sup>206</sup>

2176. In the Consent Order with the State of DFS, RBS agreed to pay to the Department, pursuant to Banking Law § 44, the amount of \$50 million USD (\$50,000,000).

2177. In the Federal Reserve Consent Order to cease and desist, RBS was required to pay an additional \$50 million USD (\$50,000,000).

2178. In addition, RBS N.V., entered into a DPA with the United States based on its illegal conduct. RBS N.V. agreed the following facts are true and correct:

- a) From in or about 1995 through in or about December 2005, RBS N.V., through a number of its branches, offices, subsidiaries, and affiliates, violated the laws of the United States by systematically executing payment messages designed to circumvent and evade detection by OFAC filters at financial institutions in the United States in order to move hundreds of millions of dollars illegally through the U.S. financial system on behalf of sanctioned entities, including Iran.
- b) In doing so, RBS N.V. altered and falsified SWIFT payment messages for sanctioned entities including Iran, and used cover payments.

---

<sup>206</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order, as if fully set forth herein.

- c) Further, RBS N.V. provided special services in instructions to the sectioned entities to ensure that payments in violation of U.S. laws and regulations, cleared through U.S. financial institutions. They did this by:
  - i. removing names and references to sanctioned entities from payment messages;
  - ii. altering the names of the sanctioned entities;
  - iii. instructing the sanctioned entities to include the code word “SPARE” in their payment messages so RBS N.V. could first segregate these messages from normal message payment processing and then amend the message by removing/altering any potentially problematic text;
  - iv. creating a manual queue to ensure certain payment methods and language were used to effectuate the sanctioned payments;
  - v. replacing the names of sanctioned entities with RBS N.V. on letters of credit and foreign exchange transactions; and
  - vi. adding to payment manuals the “Special Conditions” that were to be used or certain sanctioned entities in order to circumvent the laws of the United States.
- d) In addition, RBS N.V. used these same procedures for sanctioned entities with respect to letters of credit, and the processing of USD checks and traveler’s checks.
- e) RBS N.V. undertook these financial transactions and services totaling in the hundreds of millions of USD, in and through the United States, with an intent to evade and circumvent the Iranian and other sanctions and regulations of OFAC.
- f) As part of its criminal conduct, RBS N.V. caused financial institutions in the United States to process transactions involving sanctioned entities, including banks from Iran, that the U.S. financial institutions would not otherwise have processed and prevented financial institutions in the United States from filing required banking reports with U.S. authorities.
- g) From in or about January 1998, and continuing until in or about December 2005, RBS N.V., through the New York Branch, willfully failed to establish and implement an adequate BSA/AML compliance program or to conduct appropriate due diligence on foreign correspondent accounts.
- h) Despite the institution of improved controls by RBS N.V. and its subsidiaries and affiliates, additional transactions involving sanctioned entities, including Iran,

occurred from approximately January 2006 through approximately December 2007.

- i) During these Relevant Periods, financial transactions in an amount in excess of \$500,000,000 were conducted in and through the United States via RBS N.V.'s branches, affiliate banks, and client accounts, which transactions violated the law.

2179. Based on this and other illegal conduct on behalf of Iran aimed at the United States financial system, RBS N.V. chose to enter into a sweeping DPA, admitting that it knowingly and willfully conspired in violation of Title 18, United States Code, Section 371 to defraud the United States and the U.S. Department of Treasury, OF AC; violated the IEEPA, Title 50, United States Code § 1705; and willfully failed to establish an adequate AML program in violation of Title 31, United States Code, Sections 5318(h) and 5322.<sup>207</sup>

2180. The DPA, which required the ongoing submission to the jurisdiction of the United States for purposes of trying to remediate the illegal actions taken on behalf of Iran and others, and to prevent such actions from happening in the future. To that end, RBS N.V. agreed:

- a) To pay to the United States \$500,000,000;
- b) To waive any challenges to the venue or jurisdiction of the United States District Court for the District of Columbia;
- c) To work in conjunction with and cooperate with the United States to ensure compliance with a host of matters required by the DPA;
- d) To accept and acknowledge responsibility for its conduct and that of its employees;
- e) To a continuing relationship with the United States and with any other federal, state or local governmental department or agency designated by the United States;
- f) To implement compliance procedures and training to identify and prevent circumvention of U.S. laws;

---

<sup>207</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPA, as if fully set forth herein.

- g) To maintain policies and procedures and controls to prevent and report money laundering;
- h) To maintain certain transaction documentation and information;
- i) To retain and disclose to the United States all relevant documents, electronic data;
- j) To be prosecuted for the crimes charged if it were to materially breach the substance of the agreement reached with the United States;
- k) To not make any public statement contradicting, excusing or justifying the conduct it admitted to in the DPA; and
- l) To include in any sales agreements for any of its operations involved in the transmission of USD a requirement the purchasing entity be bound by the terms and conditions of the DPA.

## **9. Crédit Agricole's Participation in the Conspiracy**

2181. CASA and CACIB agreed to, and participated in, the Conspiracy.

2182. CACIB and its subsidiaries (including CASA) agreed to provided Iran, Iranian entities, Iranian SDNs, and others with billions of USD, money that those entities used to finance terrorist activities, including those that injured or killed Plaintiffs. They agreed to provide USD in violation of U.S. law and sanctions put in place to prevent Iranian entities from financing terrorist activities, including those that injured or killed Plaintiffs. They participated by illegally providing billions of USD over a number of years, which ultimately supported the Terrorist Groups involved in the terrorist acts that injured or killed Plaintiffs. That participation earned CACIB and CASA a significant amount of profits. Further, CACIB and CASA engaged in these transactions fully aware the reason for the U.S. laws and sanctions they violated was to inhibit Iran's ability to fund terrorism using USD.

2183. From at least August 2003 to September 2008, CACIB had a continuous, ongoing relationship with Iran and its Agents and Proxies. CACIB's relationship with, and its illegal processing of USD transactions on behalf of, Iranian entities stretches back even further. In

addition to Iranian entities, CACIB during this period processed more than 4,000 transactions on behalf of 11 Sudanese banks, six of which were SDNs.

2184. During its review of \$32 billion of transactions during this time frame, the DFS found that more than 4,000 of those transactions, valued at approximately \$442 million, were illegal under various U.S. sanction programs. The DFS also specifically found, from the sample it reviewed, the bank processed 280 transactions totaling approximately \$50 million involving SDNs. The DFS also found that about 90% of the bank's illegal transactions (which accounted for approximately 80% of the total value of the illegal transactions) were processed by the bank's Geneva subsidiary.

2185. During this time, CACIB and its subsidiaries (including CASA), predecessors and affiliates, systematically and repeatedly violated U.S. and New York law by sending prohibited USD payment transactions through its branch in New York on behalf of Iran and Iranian entities. To accomplish this goal, CACIB and its subsidiaries and predecessors designed these payments to hide the fact payments were requested by Iran or Iranian entities to avoid detection by both United States banking personnel and United States and New York regulators and law enforcement.

2186. From at least 2003 to 2008, CACIB used a series of schemes to process more than \$32 billion in U.S. dollar payments through its New York Branch from its branches in Paris, London, Singapore, Geneva, Hong Kong and the Gulf, providing U.S. dollar clearing services on behalf of Sudanese, Iranian, Burmese and Cuban entities, including SDNs. From at least August 1, 2003 to September 1, 2008, CACIB transferred at least \$312,000,000 in transactions on behalf of Iranian entities and other sanctioned persons in violation of U.S. sanctions.

2187. Specifically, CACIB and its subsidiaries and predecessors (1) sent USD payment transactions through the United States on behalf of Iran and Iranian entities without reference to the payment requestor's origin, (2) eliminated payment data from USD transactions that would have revealed the involvement of Iran or Iranian entities, and (3) used alternative USD payment methods to mask the involvement of Iran and Iranian entities.

2188. CACIB engaged in billions of dollars of transactions involving Iran while it was the bank's policy to not disclose the Iranian connection of these transactions to authorities in the United States, as detailed further below. Internal procedures at CACIB, found by the DFS investigation, stated that CACIB had been "dealing with these [Iranian] counterparts for over 14 years" and, like "all our competitors in this market," were stripping wire information from USD transactions sent through the United States "in order to prevent funds being seized by the US authorities." CACIB policy during this time instructed those within CACIB to send payment messages to the United States "**WITH NO MENTION OF IRAN.**" An internal CACIB memorandum cautioned staff in 2005 that "no mention of Iran is made" in the payment messages transiting through the United States and that "we have been routing USD payments in the manner specified below in order to prevent funds being seized by the U.S. authorities."

2189. At least by 2002, CLS, a predecessor to CACIB, was routing payment messages through a bank branch in New York that omitted references to Iranian parties and instead referred the ordering party as "one of our customers." In 2004, a CLS senior back office manager disseminated a policy that required the ordering party be reflected on payment messages, except when a risk of embargo was possible, in which case the bank stripped the client information from the messages and often replaced it with ambiguous phrases such as "one of our clients" or "our good customer." Other CACIB entities employed the same tactic during the same timeframe.

2190. Specifically, the bank instructed employees to “send a separate MT 202 (bank to bank transfer) to our NY correspondent instructing the transfer of USD xxx to the NY correspondent of the receiver of the MT 103. No mention on this message of payment to any Iranian counterpart or beneficiary. This, the message containing the ‘Iranian details,’ is not sent to the U.S.” Thus, CACIB would generally process outgoing USD payments on behalf of its Iranian clients by generating an MT 103 payment message destined for the non-U.S. beneficiary with complete information related to the transaction’s parties as well as an MT 202 cover payment destined for the intermediary U.S. financial institution that did not include the names of any Iranian entities. CACIB’s New York branch knew, or was deliberately and/or recklessly indifferent to these facts.

2191. The various bank departments were aware of “this special treatment.” As the DFS found, “it was the policy of the Bank, as directed by its compliance professionals, to intentionally omit Sudanese, Iranian, Burmese or Cuban information from U.S. dollar denominated payment messages.” The bank engaged in this conduct even though it knew it was illegal, as explained by a 2005 internal memorandum: “Iran is subject to an embargo from OFAC [] of the U.S. Treasury Department. This embargo is applicable directly to all ‘US persons’ and indirectly to all transactions denominated in USD even when performed out of the United States.”

2192. Through this conduct, CACIB and its subsidiaries and predecessors (1) prevented detection by United States and New York regulators and law enforcement, (2) prevented United States and New York financial institutions from filing reports required by the United States government and state of New York, (3) caused false information to be recorded in the records of United States and New York financial institutions, (4) caused United States and New York financial institutions to not make records that should have been made as required by United

States and New York law, and (5) caused false entries to be made in the business records of financial institutions located in the United States and the state of New York.

2193. Based on this conduct, CACIB was charged by the DOJ with violating the Trading with the Enemies Act (18 U.S.C. § 371) by conspiring to commit violations of regulations prohibiting the export of services to Iran and Iranian entities from the United States.

2194. CACIB, through Crédit Agricole (Suisse) SA (“CAS”) and its predecessor entities, intentionally used non-transparent methods for payment messages, as described above, to conceal the involvement of sanctioned entities and SDNs in USD transactions processed in the United States. CACIB, through CAS and its predecessor entities, engaged in those acts with the specific intent to evade U.S. sanctions. The Conspiracy was successful, in part, because the massive number of lawful USD payments that CACIB processed made it easier for the unlawful payments to go unnoticed.

2195. CACIB was also charged by the state of New York with violations of New York State Penal law 175.05, 3 N.R.C.R.R. § 3.1 for falsifying business records, and failing to maintain accurate books, accounts and records as required by New York Banking Law§ 200-c.

2196. CACIB also entered into a settlement agreement with the United States Department of the Treasury, relying on the same factual predicate of consistent and widespread abuse of the United States financial system on behalf of Iranian entities that served as the basis for the DOJ and the DFS actions taken. While CACIB, and its predecessors, engaged in billions of dollars of transactions with Iranian entities over many years, OFAC specifically identified sixteen electronic funds transfers in the aggregate amount of \$397,453 from October 2003 to December 2006 to or through financial institutions located in the United States in apparent

violation of the prohibition against the exportation or re-exportation of services from the United States to Iran, 31 C.F.R. § 560.204.

2197. CACIB entered into a DPA with the DOJ and OFAC in 2015, agreeing to hundreds of millions of dollars in fines for violating U.S. sanctions, including sanctions on Iran.<sup>208</sup>

2198. In resolution of these charges, CACIB admitted to certain facts which are examples of the extent to which CACIB and its subsidiaries, predecessors, and affiliates conducted illegal transactions utilizing the United States financial system.

2199. For example, from at least in or around August 2003 up through and including September 2008, CACIB, through its subsidiary in Switzerland, CAS, and its predecessor entities, Crédit Agricole Indosuez (Suisse) SA (“CAIS”) and CLS, violated U.S. laws by sending prohibited payments through the U.S. financial system on behalf of entities subject to U.S. economic sanctions. In an effort to evade detection by U.S. bank personnel as well as U.S. authorities, CAS and its predecessor entities knowingly, intentionally, and willfully concealed the sanctioned entities’ involvement with these transactions. Consequently, U.S. financial institutions processed transactions that otherwise should have been rejected, blocked, or stopped for investigation pursuant to regulations promulgated by OFAC relating to transactions involving sanctioned countries and parties.

2200. The conduct of CAS and its predecessor entities included, among other things, (i) sending payments on behalf of sanctioned customers without reference to the payments’ origin; (ii) eliminating payment data that would have revealed the involvement of sanctioned countries

---

<sup>208</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPAs, as if fully set forth herein.

with the specific intent to evade U.S. sanctions; and (iii) using alternative payment methods to mask the involvement of sanctioned entities, including the use of two payment messages, for payments involving sanctioned financial institutions that were sent to the United States.

2201. By providing banking services on behalf of sanctioned entities, CAS and its predecessor entities: (i) prevented detection by U.S. regulatory and law enforcement authorities of financial transactions that violated U.S. sanctions; (ii) prevented U.S. financial institutions from filing required reports with the U.S. government; (iii) caused false information to be recorded in the records of U.S. financial institutions; (iv) caused U.S. financial institutions not to make records they otherwise would have been required by U.S. law to make; and (v) caused false entries to be made in the business records of financial institutions located in the United States. These payment methods deceived U.S. financial institutions and created the false appearance the transactions had no connection to sanctioned entities.

2202. During the Relevant Period, CACIB typically executed and processed international U.S. dollar denominated wire payments on behalf of clients in two ways. The first method, known as a “serial payment,” was to send a single message, commonly referred to as an MT 103, to each financial institution in the transmission chain, identifying the originator and beneficiary of the USD denominated payment. The second method, known as a “cover payment” involved sending two SWIFT messages in connection with a single payment. In the cover payment method, one message—typically an MT 103—identifying the originating customer and beneficiary of the payment, was sent directly from the customer’s bank (i.e., Foreign Bank A) to the ultimate beneficiary’s bank (i.e., Foreign Bank B) while a second message—typically an MT 202—identifying only the originating bank (but not the customer or the beneficiary) accompanied the funds as they transferred through the United States. During the Relevant

Period, cover payment messages typically did not require the sending bank to identify the party originating a payment or its ultimate beneficiary, whereas serial payment messages did.

2203. Financial institutions in the United States that process U.S. dollar transactions from overseas, including CACIB's branch in New York ("CACIB NY"), are expected to screen financial transactions, including international wire payments effected through the use of SWIFT messages, to ensure such transactions do not violate U.S. sanctions. Because of the vast volume of wire payments processed by financial institutions in the United States, most institutions employ sophisticated computer software, commonly referred to as filters, to automatically screen all wire payment messages against a list of sanctioned entities. When the filters detect a possible match to a sanctioned entity, the payment is stopped and held for further manual review. When a financial institution detects a transaction that violates sanctions, the institution must "reject" the payment—that is, refuse to process or execute the payment and notify OFAC of the attempted transaction. If a party to the payment is an SDN, then the payment must be frozen or "blocked" and the bank must notify OFAC. The sending bank must then demonstrate to OFAC the payment does not violate sanctions before the funds can be released and the payment processed.

2204. During the Relevant Period, CACIB NY utilized an automated OFAC filter that screened all incoming MT 103 and MT 202 payment messages, including all USD denominated payment messages sent by CAS and other CACIB branches, to identify both SDNs and companies owned or controlled by SDNs, or persons located in targeted countries. CLS, CAIS, and CAS, for the duration of the Relevant Period, failed to conduct comprehensive filtering akin to the type of filtering conducted by CACIB NY. After September 11, 2001, in accordance with Swiss regulations, CLS and CAIS added terrorists designated by OFAC—a subset of the SDN List—to their filters. However, CAS did not actually filter against the complete SDN List until

after September 2005. And it was not until 2008 that CAS began filtering transactions to identify, in a comprehensive fashion, entities involved in transactions that were owned by, controlled by, or located in targeted countries, including Iran.

2205. The practice of omitting or removing sanctions-identifying information in outbound USD payment messages was spread to multiple business lines throughout the bank and was noted in a February 2, 2004 notice written by a CAIS Back Office Analyst:

Various payments of ours were stopped by the U.S. banks, because within the text body of our instructions (MTI 03 or 202), certain words such as Iraq, Iran, etc. were used, words which appear on the U.S. Banks [sic] automatic block list. Consequently, be vigilant and do not put too much detailed information in your payments, thus avoiding costly back values.

2206. CAIS (and subsequently CAS) continued to receive numerous indications that its interpretation of U.S. sanctions laws was incorrect. For example, CACIB's New York branch blocked or rejected a number of transactions originated by CAS for processing and provided CAS with additional information regarding U.S. sanctions, informed the Head Office of such issues and suggested additional sanctions-related training. Later, on December 1, 2005, a Compliance employee from CACIB's Head Office in Paris distributed a memorandum describing the group's policy with regard to Iran. The memorandum included statements suggesting that CAS's understanding of U.S. sanctions was incorrect, including: "Iran is subject to an embargo from OFAC [] of the U.S. Treasury Department. This embargo is applicable directly to all 'US persons' and indirectly to all transactions denominated in USD even when performed out of the United States." Despite receiving these warnings, CAS did not seek clarification from either its Head Office or its New York branch regarding the applicability of OFAC sanctions to CAS.

2207. With full understanding of the improper nature of its conduct, in September 2005, CACIB London drafted a memorandum entitled Special Treatment of Iranian Related Payments/Operational Risk that directed that “no mention of Iran” should be “made on [the MT 202 cover payment]” to the U.S. correspondent banks. The memo noted the knowledge of “the various departments involved in this process i.e. front, middle and the back-office … of this special treatment as procedures have been implemented to cover this aspect of operational risk.” A separate cover memo to the memo stated that this matter had been vetted “through Compliance and Legal to ensure that all aspects are covered. . . The method for [USD] payments is as follows: no mention of Iran is made on this instruction.”

2208. In particular, the memo stated the bank had been “routing USD payments” in a manner that “prevent[ed] funds being seized by the U.S. authorities.” Not surprisingly, personnel within the CACIB network viewed this policy as CACIB memorializing a procedure for circumventing U.S. sanctions. For example, in a February 2006 email to a senior compliance officer at CAS, a senior manager within the Monitoring and Investigations Unit (“MOIN”) noted “[a]lthough a note has been drawn up by the Group in particular for transactions in USD with Iran as the destination (commercial transactions/oil), the question finally arises of the implementation of a payments system allowing the US embargo rules **to be got around.**” (Emphasis added).

2209. Furthermore, on March 21, 2007, a Head Office Financial Security employee wrote in an email to another employee, “…on the express condition the goods are never of Iranian origin or manufacture-this does not fall within the scope of the note. However, it is evident that in the event of flows and therefore of SWIFT’s references to IRAN in the free fields must be avoided, so as not to have to provide lengthy justification to the Yankee authorities.” On

March 22, 2007, the same employee approved an otherwise permissible U-turn transaction regarding goods of Iranian origin owned by a Turkish company if there was “No reference to the country of origin in the SWIFT 10X or 20X messages.”

2210. Compliance staff in the Geneva branch actually developed a presentation detailing how to conceal USD transactions for Iran and Iranian entities: “Transfer instructions (MT 202) sent to Bank A’s U.S. correspondent **WITH NO MENTION OF IRAN**. . . no reference to Iran is made regarding this transaction.” (Emphasis in bold added).

2211. Similar instructions were circulated in the head office in Paris: “[w]e send a separate MT 202 (bank to bank transfer) to our NY correspondent instructing the transfer of USD xxx to the NY correspondent of the receiver of the MT 103. No mention is made on this message of payment to an Iranian counterpart or beneficiary. Thus, the message containing the “Iranian details” is not sent to the US.”

2212. Similarly, in October 2005, an employee at CACIB Dubai—in response to press reports of RBS’s U.S. sanctions violations—referenced the use of cover payments for Iranian payments, specifically noting the MT 202 message was to be sent “without mentioning the name of the Iranian Bank, or any related reference to the concerned transaction,” and questioned whether CACIB’s practices were lawful. This email was ultimately forwarded to compliance personnel at CACIB NY, who promptly raised the issue with CACIB’s compliance department in Paris. In the course of raising concerns, a compliance officer at CACIB NY explained the email raised concerns that “stripping” was occurring within the Bank’s network.

2213. On January 31, 2006, another CACIB NY compliance officer questioned the lack of transparency with cover payments, asking a senior manager responsible for compliance at CACIB Paris whether CACIB policy prohibited bank personnel from noting in MT 202s whether

the bank-to-bank payment was related to an underlying customer payment (i.e., an MT 103). The senior manager from CACIB Paris responded, stating that Paris reviewed and approved Iranian-related USD payments and that bank personnel were not precluded from noting that an MT 202 was related to an MT 103. But the senior manager failed to disclose that, for Iranian payments, CACIB Paris had a policy that precluded CACIB from mentioning Iran in messages sent through the United States related to U-turn payments. Accordingly, while CACIB NY Compliance personnel had the broadest knowledge of U.S. sanctions of any personnel within the CASA network, CACIB's, CLS's, CAIS's, and CAS's policies, procedures and/or practices for processing international payments involving sanctioned countries or entities removed CACIB NY compliance personnel, their filter, and their expertise from the review process.

2214. In 2003, CAIS's Compliance department was divided into two groups: (1) Legal and Compliance, and (2) the MOIN. Both were under the supervision of the Office of the General Secretary. Prior to 2004, Legal and Compliance had responsibility for U.S. sanctions compliance, meaning the business lines and operational units turned to, and relied upon, Legal and Compliance for guidance. In 2004, this responsibility was shifted from Legal and Compliance to MOIN.

2215. Throughout the Relevant Period, certain CAIS and CAS personnel, including personnel within Legal and Compliance and MOIN, knew that U.S. sanctions laws applied to transactions that CAIS and CAS sent through the United States.

2216. CAS developed policies and procedures to use cover payments (i.e., MT 202 messages) which did not reference any sanctioned entity's involvement in transactions, fully recognizing that this payment method would conceal the fact these transactions concerned sanctioned parties. CAS did not share its policies and procedures for processing international

payments with CACIB NY, and CACIB NY lacked access to CAS's systems that contained these policies and procedures.

2217. As early as 2001, an attorney who was part of CAIS's management team sent an email to a CACIB employee based in Paris, which stated that "to the extent the process used by our establishment via our U.S. correspondent bank ([U.S. Bank 1]), and whereby our establishment erroneously misleads the latter as to the real beneficiary for the transfers...and by the designation of an institutional beneficiary instead and in place of the actual one...whose identity [the U.S. correspondent] is unaware, we could expose ourselves to various sanctions in the USA. To our knowledge, the majority of the Group entities operate in the same manner."

2218. In 2004, when responsibilities for U.S. sanctions compliance were shifted to MOIN, the group required all transactions concerning countries subject to U.S. sanctions, and sanctions imposed by other jurisdictions, to be forwarded to MOIN for review and authorization.

2219. As early as June 10, 2004—shortly after this shift—a senior manager within MOIN, after noting in an email that "the reach of the American sanctions is . . . limited" and only applied to the "American territory," acknowledged that a payment involving a sanctioned entity that transited through the United States could potentially be blocked if the U.S. clearer learned of the existence of the sanctioned entity.

2220. Beginning in April 2005, a senior manager within MOIN commonly acknowledged in emails that U.S. sanctions applied to transactions that were sent through the United States: "OFAC (United States) has taken economic sanctions against Sudan and Iran for transactions which occur on U.S. territory and/or which are made out in Dollars and/or for which U.S. companies and individuals appear . . . and for which individual approval must be obtained

from the U.S. authorities.” This language demonstrates that certain CAS employees knew that U.S. sanctions applied to transactions that transited through the United States.

2221. In and around 2006, MOIN’s own compliance materials acknowledged the “extra-territorial reach” of U.S. sanctions laws and that these laws cover “all investments and transactions in the United States or that involve a U.S. person anywhere in the world.”

2222. On or about February 2, 2006, the Office of the General Secretary drafted a memorandum that stated, “the simple fact of using a clearing bank in the United States requires complying with [anti-money laundering and OFAC] rules.”

2223. Despite this knowledge, MOIN authorized many of the USD transactions forwarded to them, even though they violated U.S. sanctions, often precisely because the payment messages that were going to be sent to the United States would not reference a sanctioned entity’s involvement in a transaction. The clear intent of ensuring that payment messages sent to the United States did not reflect information about sanctioned entities is reflected in a series of communications regarding two transactions that were rejected on or about March 29, 2006. After CACIB NY notified a senior manager within the Office of the General Secretary of the rejected payments, the senior manager raised these rejected payments with a senior manager within MOIN and another member of MOIN. Rather than asking how payments that violated sanctions were sent to the United States, the senior manager within the Office of the General Secretary questioned why MT 103s were sent in connection with the payments and why CAS’s systems that were processing payments involving sanctioned entities used this message type (a message type that would clearly reveal the involvement of sanctioned entities). When the senior manager within MOIN reported the back office sent MT 202 messages to CACIB NY containing the ordering party’s name and that CACIB NY learned of the Sudanese connection to

the transactions through its own due diligence, CAS personnel complained about the heightened due diligence from their U.S. counterparts. No one within CAS took any steps, at that time, to stop all USD MT 202 payments involving sanctioned entities that cleared through the United States.

2224. Instead, MOIN authorized a number of other transactions involving sanctioned entities to transit through the United States while emphasizing payment messages that would be sent through the United States did not reference Sudan. For example, in March 2006, in an email copying a senior manager within the Office of the General Secretary, MOIN authorized a LC for a Sudanese SDN bank, one of which was not on the SDN List, but was considered an SDN by operation of law. Specifically, the email stated that “at no moment shall information related to the transactions as such (End Beneficiary/Counterparty/End Bank) be transmitted/indicated within the aforementioned messages in accordance with what is acceptable under U.S. regulations.” MOIN authorized the transaction despite the fact less than a year earlier CACIB NY rejected a nearly half-million dollar payment involving this Sudanese bank.

2225. CAS also employed the practice of replacing client information on payment messages with ambiguous phrases such as, “one of our clients” and “our good customer.” The practice continued despite the fact CACIB NY had entered into a Commitment Letter in September 2005 with the Federal Reserve Bank of New York and the DFS (then the New York State Banking Department) in which it committed to enhance its AML and Bank Secrecy Act functions.

2226. In December 2006, the Head Office decided to diversify USD clearing banks and CAS started using a non-affiliated bank based in the United States as its exclusive clearer. After establishing a relationship with a new clearing bank, MOIN persisted in approving transactions

involving sanctioned entities, so long as messages that were sent to the United States did not reveal the involvement of the sanctioned entities.

2227. In total, from approximately August 2003 through approximately September 2008, CLS and CAIS, and later CAS, processed at least \$312 million in payments in violation of U.S. sanctions laws.

2228. CLS maintained a policy dating back to 2002 to utilize cover payments for outgoing USD Iranian-related transactions. In June 2002, CLS New York sent an inquiry to CLS Paris in relation to an outgoing transaction the latter had originated that referenced the ordering party as “one of our customers.” CLS Paris’s Head Office Financial Security subsequently identified the originator as an Iranian party and sought legal guidance from external counsel. The bank noted that its external counsel drafted a legal memorandum in October 2002 regarding U.S. sanctions laws, including the U-turn rule. Thereafter, Credit Lyonnais’ Financial Security department determined that cover payments were part-and-parcel of the U-turn rule and Credit Lyonnais used cover payments to process U-turns involving Iranian corporate entities. This informal policy was maintained by CACIB Financial Security after the merger, as the unit was largely comprised of the former compliance personnel from CLS Paris. As a result, throughout the review period, CACIB would generally process outgoing USD payments on behalf of its Iranian clients by generating a SWIFT MT 103 payment message destined for the non-U.S. beneficiary financial institution with complete information related to the transaction’s parties, and a SWIFT MT 202 cover payment destined for the intermediary U.S. financial institution that did not include the names of any Iranian banks and/or persons.

2229. Prior to the merger between CLS and Crédit Agricole Indosuez, Crédit Agricole Indosuez Paris’s branch processed Iranian-related capital market transactions (i.e., treasury and

foreign exchange transactions) with direct SWIFT MT 202s with the account number of the Iranian bank listed in Field 72. The Paris system would send a SWIFT MT 210 (Notice to Receive) message to the U.S. clearing bank which included the SWIFT BIC of the Iranian bank. Following the merger, the bank's Capital Markets unit requested guidance from Head Office Financial Security regarding these types of transactions. In response, the Head Office Financial Security instructed the Capital Markets unit to begin processing its transactions by using cover payments in the same manner described above (i.e., using an outgoing SWIFT MT 103 and SWIFT MT 202). Although the Capital Markets unit questioned these instructions, the Financial Security department confirmed its instruction, indicating the use of cover payments for Iranian transactions was supported by the October 2002 legal memo received by external counsel.

2230. The practice of utilizing cover payments for Iranian-related payments was not officially adopted as policy until late 2005, in or around the time at which various U.S. regulatory authorities were preparing to announce a settlement with Defendant and co-conspirator RBS in response to its violations of U.S. economic sanctions (including several related to Iran). The policy adopted by CACIB emphasized that “no mention of Iran” should be “made on the [SWIFT MT202 cover payment.]” At least sixteen Iranian-related transactions did not meet the terms of the U-turn general license and constituted apparent violations of the Iranian Transactions and Sanctions Regulations.

2231. From October 2003 to December 2006, CACIB, including its subsidiaries and their predecessors, processed 16 electronic funds transfers in the aggregate amount of \$397,453 to or through financial institutions located in the United States in apparent violation of the prohibition against the exportation or re-exportation of services from the United States to Iran, 31 C.F.R. § 560.204.

2232. The conduct of CACIB and its predecessors was not based on a mistaken assumption, but was intentional.

2233. As a result of this knowing exploitation of the United States financial system for its own benefit and the benefit of its Iranian customers, CACIB entered into a DPA with the DOJ to be overseen by the United States District Court for the District of Columbia.

2234. This DPA resulted in the forfeiture of \$312 million dollars to the United States government by CACIB, a portion of which was directly attributable to the illegal USD transactions on behalf of Iran.

2235. In this DPA, CACIB and its subsidiaries subjected itself to the continuing jurisdiction of the DOJ and the United States District Court for the District of Columbia for three years. This level of oversight, directly related to the manipulation of the United States financial system on behalf of sanctioned Iranian entities, consisted of:

- a) CACIB must cooperate with the Department of Justice and any other United States law enforcement or regulatory agency in any investigation into CACIB and its subsidiaries and predecessors' involvement in the illegal laundering of funds on behalf of Iran and Iranian entities;
- b) CACIB must make employees available to United States law enforcement officials for interview or testimony related to this investigation;
- c) CACIB must provide United States law enforcement officials with all documents and information necessary to authenticate documents and information for purposes of admitting such document or information into evidence in a judicial proceeding; and
- d) CACIB must implement a compliance and ethics program designed to prevent and detect USD payment transactions sought on behalf of sanctioned entities, including Iran and Iranian entities. The terms of this compliance agreement are broad, requiring CACIB to:
  - i. Apply a current and complete OFAC sanctions list against all USD transactions, including both incoming and outgoing payment messages;

- ii. Specifically agree to not undertake any USD transaction for Iran or any Iranian entity;
- iii. Complete Financial Economic Crime sanction training addressing United States sanction and trade control laws for all employees;
- iv. Require the use of SWIFT MT 202COV bank-to-bank payment messages that strictly adhere to the SWIFT guidelines;
- v. Implement compliance and training designed to ensure the CACIB compliance officer is timely made aware of known requests or attempts by any entity to omit its name or obscure identifying information in an attempt to evade United States sanction law;
- vi. Maintain all SWIFT payment messages and all documents and material produced by the company to the DOJ for the duration of the DPA;
- vii. Abide by all measures and actions required by OFAC as a result a settlement reached between OFAC and CACIB in October of 2015;
- viii. Abide by all measures and requirements of the settlement agreement reached between CACIB and the DFS;
- ix. Provide the Department of Justice with all reports, disclosures and information that CACIB provides to any other governmental entity as a result of any such agency's investigation into CACIB's conduct with respect to sanctioned entities and USD payment transactions;
- x. Notify the United States of any criminal, administrative or regulatory investigation commenced against it or any of its executives or personnel;
- xi. Report to the Department of Justice every 90 days during the term of the three-year period of the agreement consisting of detailed accounts of CACIB's compliance with all aspects of the agreement;
- xii. Agree that it would be subject to federal prosecution in the United States District Court for the District of Columbia should it breach the terms of the agreement, without regard to the statute of limitation;
- xiii. At the conclusion of the three-year period, the Head of Compliance must certify its compliance to the DOJ;
- xiv. Transfer the material obligations of the agreement to any purchaser of the company; and

xv. Not make any public statement that is inconsistent with the admissions contained in, or obligations undertaken by, entering into the agreement.

2236. In addition to the terms of the formal DPA, CACIB voluntarily undertook the following steps as a result of the investigation to enhance and optimize its compliance program in an effort to avoid further violations of United States law and regulation:

- a) Install more sophisticated filtering software;
- b) Create more compliance-focused groups to address sanctions compliance and correspondent bank due diligence;
- c) Hiring additional compliance employees; and
- d) Adopting written compliance policies that address United States sanctions against Iran and other sanctioned entities.

2237. CACIB and CASA also entered into a Consent Order with the DFS based on its rampant processing of illegal USD transactions on behalf of Iran and Iranian entities.<sup>209</sup> In this Consent Order, CACIB and CASA were required to submit to the jurisdiction of the state of New York for implementation of the following conditions of its deferred prosecution:

- a) CACIB and CASA paid a \$385,000,000 penalty to the DFS, a portion of which was directly attributable to the illegal transactions processed on behalf of Iranian entities;
- b) Terminate a specific bank employee;
- c) Hire an independent consultant, at their own expense, dictated by the state of New York, for the term of one year to conduct a comprehensive review of the compliance programs, policies and procedures at the CACIB New York branch and its other branches throughout Europe that deal with USD transactions conducted through New York;
- d) CACIB and CASA are required to fully cooperate with the consultant and provide access to all personnel, documents and other items necessary in any of its locations;

---

<sup>209</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Consent Order, as if fully set forth herein.

- e) In response to the consultant's report at the conclusion of its investigation, CACIB and CASA will be required to submit a Management Oversight Plan to the state of New York to address concerns raised by the consultant's report;
- f) The independent consultant would oversee the implementation of any corrective measures identified by the Management Oversight Plan; and
- g) The independent consultant will also be responsible for assessing CACIB and CASA's compliance with the Management Oversight Plan and will be required to submit progress reports to the state of New York.

2238. In terms of its Settlement Agreement with OFAC,<sup>210</sup> based on the conduct set forth above, CACIB agreed:

- a) To a contingent fine in the amount of \$329,593,585 in the event that amount levied against it by the Department of Justice and the DFS was less than that sum;
- b) That it had terminated, among other things, all of the illegal conduct described herein with respect to Iran and other sanctioned entities;
- c) That it would maintain policies and procedure resulting from the agreements with the Department of Justice and the state of New York that would minimize, and prohibit if possible, the risk of similar conduct in the future; and
- d) To provide the Department of the Treasury copies of all reports submitted to the United States Federal Reserve relating to its illegal conduct described herein.

## **10. Credit Suisse's Participation in the Conspiracy**

2239. Credit Suisse agreed to, and participated in, the Conspiracy.

2240. During the Relevant Period, Credit Suisse had a continuous, ongoing relationship with Iran and its Agents and Proxies.

2241. Credit Suisse provided special services to ensure that payments in violation of IEEPA and OFAC regulations for Iran, Sudan, Burma, Cuba, and Libya cleared through U.S.

---

<sup>210</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the Settlement Agreement, as if fully set forth herein.

financial institutions. The total value of these transactions reviewed by the Department of Justice exceeded \$1.6 billion.

2242. From at least August 19, 2003 to November 1, 2006, Credit Suisse transferred at least \$480,072,032.00 in 4,775 transactions on behalf of Iranian entities and persons in violation of U.S. sanctions, including Iranian sanctioned entities.

2243. Credit Suisse intentionally processed these illegal transactions in such a manner as to avoid detection by United States regulators and law enforcement. In particular, Credit Suisse removed identifying information about Iran and Iranian entities from the SWIFT payment messages, used non-transparent cover payment methods that were stripped of important identifying information about the underlying party, and instructed Iranian clients to include notes or code words in requested payment transactions that would trigger special processing by Credit Suisse employees to ensure Credit Suisse employees would hide identifying information to avoid having the payment requests picked up by U.S. based Credit Suisse personnel and OFAC filter software.

2244. As a result of this conduct, Credit Suisse failed to maintain, and caused other banks to fail to maintain, adequate and correct financial records of USD payment transactions and the omitted and modified payment requests set forth above likewise prevented Credit Suisse and other banks from maintaining adequate and complete financial records as required by state and federal law.

2245. Like the other Defendants in this action, Credit Suisse worked hand-in-glove with Iran and Iranian Bank co-conspirators acting at Iran's behest to develop procedures to structure USD payments in ways that would evade U.S. sanctions and leave U.S. regulators, law enforcement and financial institutions blind as to Iran's financial activities.

2246. To this end, Credit Suisse worked diligently to (1) develop methods that would avoid disclosing the true originators and/or beneficiaries of Iranian transactions that it was clearing and settling in the United States; (2) delete or omit certain information when transactions were to be processed through the United States; and (3) provide incorrect information in USD funds transfer instructions executed through the United States on behalf of U.S.-sanctioned individuals and entities.

2247. Credit Suisse worked closely with Bank Melli, Bank Saderat, and Iran's Atomic Energy Organization (and other designated WMDs proliferators) for many years.

2248. Before 2003, Credit Suisse was an active participant in the Conspiracy, but the sheer volume of its illegal conduct accelerated greatly in 2003 when Lloyds exited its Iran business and Bank Melli Plc, Defendant Bank Saderat, and other Iranian Agents and Proxies moved their accounts to Credit Suisse.

2249. For the next two years, Credit Suisse became one of the main USD funds clearing banks for the Iranian banking system, quadrupling in only 3 years the number of Iranian USD payments, from approximately 49,000 in 2002 to nearly 200,000 in 2005.

2250. The procedures Credit Suisse developed and refined over time to assist Iran were embodied in internal directives, memoranda, emails between Credit Suisse and its Iranian bank clients and internal e-mails involving, among others, a Credit Suisse Bank Payments Sector Head, Credit Suisse's Treasury and Trade Finance Departments, and the Head of Credit Suisse's Iran Desk.

2251. Since at least the mid-1990s, when it first agreed to assist Iran in carrying out the Conspiracy, Credit Suisse's Iran Desk began adding internal warnings to the accounts of its

Iranian bank clients, instructing Credit Suisse employees: “Do not mention the name of the Iranian bank in payment orders.”

2252. Such warnings ensured that payment orders given by the Iranian Bank co-conspirators would not be processed automatically, but rather would be manually reviewed, “corrected” if necessary, and effectuated by Credit Suisse employees.

2253. For example, in June 1995, the Credit Suisse representative office in Dubai, UAE, issued a memorandum recognizing Iran and the Iranian bank’s general scheme to ensure that any foreign banks the Iranian Bank co-conspirators did business with masked their transactions, and accordingly advised:

Following the decision by the American authorities to declare a unilateral embargo against the Islamic Republic of Iran on April 30th, (an Iranian bank) approached Credit Suisse to open (a type of correspondent banking account for USD transactions). Crucial to them was that the name of the bank would not be mentioned on the transfer orders... Subsequently, (the Iranian bank) was informed that though payments in such a way are basically feasible, to omit the name of the bank could lead to some problems. Meanwhile, operations through this account have started... Some transfers have been rejected by the American banks as the name of (the Iranian bank) appears under the rubric ‘Ordering Bank.’ Question: a) what can be done to avoid this?

2254. Almost immediately after President Clinton issued E.O. Nos. 12957, 12959, and 13059, which strengthened existing U.S. sanctions against Iran, the Iranian Bank co-conspirators began requesting that Credit Suisse omit their names and BICs from payment messages Credit Suisse sent to its U.S. correspondent banks.

2255. Credit Suisse complied with the Iranian Bank co-conspirators’ illegal requests and purposefully omitted their names and identifiers in order to help bypass U.S. financial institutions’ sanctions filters.

2256. After a 1998 corporate reorganization, in order to further its ongoing efforts to evade U.S. sanctions and ensure that other U.S. financial institutions would automatically

process this new stream of payments, Credit Suisse notified its Iranian clients about the change in USD funds clearing and settlement from Credit Suisse First Boston AG to third-party U.S. correspondents, and provided them with a pamphlet entitled “How to transfer USD payments.”

2257. The pamphlet provided detailed payment order formatting instructions for USD funds transfers on how to avoid triggering U.S. OFAC sanction screening filters.

2258. In a 1998 letter to an Iranian Bank co-conspirator explaining the transfer of its USD clearing services to the Bank of New York, New York, Defendants Credit Suisse wrote:

In order to provide your esteemed institution with our clearing services in U.S. Dollars, we have introduced a procedure to facilitate your USD payments through our clearing system. The change of our USD-clearer to Bank of New York, New York, will not affect our mutual relationship on any clearing transaction in U.S. Dollars as long as the established procedure will be followed.

2259. Beginning as early as 1995 and continuing through 2005, Credit Suisse, both internally and in coordination with the Iranian Bank co-conspirators, created procedures and guidelines to facilitate the processing of prohibited USD transactions by its U.S. correspondent banks, primarily the Bank of New York, New York.

2260. By using Credit Suisse’s internal processing system, employees manually keyed in “Order of a Customer” when Iranian payments had to be processed as serial payments through U.S. banks.

2261. This procedure was promoted at Credit Suisse, as demonstrated by an email from a Team Leader in the Bank Payments Unit: “In order to put an end, once and for all, to the discussions regarding the processing of USD payment orders of Iranian banks, I have worked out various examples that are to be considered binding for everyone.”

2262. Attached to the email were several screenshots of Credit Suisse's payment application illustrating how to format payment order messages to ensure they would pass through the U.S. financial institutions undetected by U.S. OFAC sanction screening filters.

2263. For example, one such screenshot showed all incoming payment messages listing an Iranian bank as the ordering institution in SWIFT-NET payment order message field "52" and contained the following explicit instructions: "Population of field 52 with 'one of our clients' in case of serial payments via the US."

2264. A second screenshot showed an incoming payment with the reference "without mentioning our banks name" in field 52 and contained the following instructions: "Population of field 52 with 'one of our clients' in case of serial payments."

2265. Until at least 2004, Credit Suisse's use of "Order of a Customer" was its standard procedure for processing bank payment messages involving Credit Suisse's Iranian customers.

2266. Credit Suisse's internal communications also reveal a continual dialogue about evading U.S. sanctions spanning approximately a decade, assessing how to better process Iranian transactions in order to promote and increase business from existing and future Iranian clients.

2267. In February 1999, Credit Suisse's Iran Desk added internal warnings to the Customer Information Files (or "CIFs") it maintained for the accounts of its Iranian bank customers, expressly directing Credit Suisse employees: "Do not mention the name of the Iranian bank in payment orders."

2268. Credit Suisse documented similar directives in subsequent years. For example, in 2002, another warning was loaded in the CIF that likewise stated: "FOR USD-PAYMENTS OUTSIDE CREDIT SUISSE/CS FIRST BOSTON DO NOT MENTION THE NAME OF THE IRANIAN BANK."

2269. Credit Suisse later decided to remove warnings from the CIFs and replaced them with long-term instructions concerning Iranian entities that instructed: “Execute USD payment orders always with direct order and cover payment.” These instructions explained they were intended to ensure (according to Credit Suisse’s internal documentation) that “an Iranian origin will never be named in USD payments carried out for Iranian banks (because of the US sanctions)!”

2270. An internal Credit Suisse memorandum dated March 12, 1999, stated: “Payment orders in USD can only be paid via the American clearing, if the name of the Iranian party is not mentioned (US sanctions). Otherwise, the amounts are returned by the American banks. Even though corresponding warnings have been loaded, there almost every week cases that are processed incorrectly by us.”

2271. Between 2000 and 2004, Credit Suisse’s Iran Desk provided similar instructions to its Iranian Bank co-conspirator clients via a standard letter, which stated in part: “The most important issue is that you and/or your correspondents do not mention your good bank’s name in field 52.”

2272. Credit Suisse’s Iran Desk also informed Iranian Bank co-conspirator clients that Credit Suisse would utilize cover payments to effect payments to or through the United States, stating in one memorandum, for example, “[o]ur payment department will stop all USD payments initiated by your fine bank in any case and shall be effected [by]... ‘Direct payment order and cover payment order.’”

2273. In order to prevent straight-through processing of all payment orders sent by Iranian Bank co-conspirators, Credit Suisse configured its payment system to interdict the payments for manual review.

2274. Credit Suisse employees then reviewed the payments to ensure they contained no references to Iran. If such references were detected, Credit Suisse employees would either delete the reference, or contact the Iranian Bank co-conspirators to request further instructions.

2275. Over time, Credit Suisse employees developed practices to omit information on the involvement of Iranian Bank co-conspirators, including the following:

- a) Entering in an empty field, or replacing the name of the Iranian Bank Coconspirators with, “Order of a Customer” or a similar phrase instead of the actual name of the ordering institution in SWIFT-NET payment order messages;
- b) Forwarding payment messages received from Iranian Bank Coconspirators falsely referencing “Credit Suisse” or Credit Suisse’s SWIFT-NET account code (identified by BIC address CRESCHZZ) instead of an Iranian bank as the originating institution. For example, a November 2000 email circulated by a team leader in Credit Suisse’s Bank Payments Unit contained screenshots of an incoming payment order from an Iranian bank co-conspirator in which Credit Suisse was listed as the ordering institution in field “52” of the SWIFT-NET payment message. The instructions were to make no changes to the misleading information in the SWIFT-NET message’s field “52” for serial payment messages made to U.S. financial institutions;
- c) Inserting “Credit Suisse” as the ordering institution in payments originating with an Iranian Bank Co-conspirator;
- d) Removing all references to Iranian names, addresses, cities, and telephone numbers from customer payments;
- e) Substituting abbreviations for Iranian customer names. For example, in an April 16, 2003 email, the Head of Credit Suisse’s Iran Desk wrote to the Credit Suisse representative office in Tehran, “entry to their account works when account number plus XXX is stipulated as beneficiary. What is also important of course is that applicant will give details of final beneficiary as reference for the beneficiary, then it should work;” and
- f) Converting SWIFT-NET MT 103 Messages to SWIFT-NET MT 202 Messages to hide the details of Iranian transactions, and using MT 202 cover payment messages approximately 95% of the time to facilitate outgoing customer payments involving Iran or Iranian parties.

2276. A September 24, 2003 Credit Suisse internal email sent from a team leader in Customer Payments to a Sector Head within Customer Payments, described Credit Suisse's Iranian USD processing:

The procedure is identical for all Iranian banks: 1) We attempt to send all USD payments directly to the bank of the beneficiary. Only cover payments are made through the US. In such cases, the ordering institution is not disclosed. 2) Should 1) *[sic]* not be possible (if the beneficiary bank is an American bank, or if no Swift connection or no correspondent was named), then the payment will be made though America. We make sure the ordering institution is not mentioned (this has been programmed into the system as a default) and the ordering customer has no connection to 'Iran.' 3) Should 1) and 2) not be possible, then the payment order will be forwarded to Investigations for further clarifications with the ordering institution.

2277. In addition, Credit Suisse actually instructed its Iranian Bank Co-conspirator customers on how to format USD payments so that such payments would evade U.S. sanctions and detection by automated filters used by U.S. financial institutions.

2278. Payment instructions included a letter from Credit Suisse's Iran Desk to an Iranian customer dated October 16, 2003, that stated: "This is to provide you our recommendation for the entry of funds how to handle bank-to-bank payments on your account with Credit Suisse and the following procedures should be applied in order to avoid any difficulties."

2279. In December 2003, an Iranian bank asked Credit Suisse for an additional USD account identifying the Iranian beneficiary bank only by a designated abbreviation (first letter of each word constituting the bank's name, together with the abbreviation commonly used for a type of legal entity, i.e., Plc).

2280. On January 28, 2004, Credit Suisse confirmed that it had opened the requested account, writing to the Iranian bank: "Reference is made to the various conversations and your

email, dated December 18, 2003 wherein you asked us to open a new USD account...Now, we would like to confirm the account number ....”

2281. In addition, Credit Suisse promised the Iranian Bank co-conspirators, including Bank Saderat and Bank Melli, that no messages would leave Credit Suisse without being first hand-checked by a Credit Suisse employee to ensure they had been formatted to avoid U.S. OFAC filters.

2282. Credit Suisse also took a further step in the Conspiracy beyond training the Iranian Bank co-conspirators on how to format their payment messages to evade OFAC filters; it also gave Iranian Bank co-conspirators materials to use for training other banks on how to prepare payment messages to evade U.S. OFAC filters and sanctions regimes.

2283. In August 2003, Credit Suisse reached an agreement with the London branches of a number of Iranian Bank co-conspirators to take over the banks’ London branches’ USD clearing activity.

2284. As a result of this agreement, Credit Suisse became one of the main USD clearing banks for the Iranian banking system.

2285. Through its subsidiary CSAM, Credit Suisse used code words for the Iranian Bank co-conspirators, when executing trades involving U.S. securities that were transmitted through the U.S.

2286. Credit Suisse knew that without such alterations, amendments, and code words, automated OFAC filters at U.S. clearing banks would likely halt the payment order messages and securities transactions, and, in many cases, reject or block the sanctions-related transactions and report the same to OFAC.

2287. Credit Suisse manipulated payment order messages and removed any identifying reference to sanctioned countries and entities so OFAC filters at the U.S. clearing banks would not be able to identify the transactions, and the transactions would be automatically processed without detection.

2288. In July 2004, the Swiss Federal Banking Commission issued an ordinance to implement the FATF's Special Recommendation on Terrorist Financing VII.

2289. The ordinance required the disclosure of the remitter in payment orders, and prompted Credit Suisse to issue an internal directive prohibiting the use of the "Order of a Customer" method when making international wire transfers.

2290. In April 2004, in preparation for the implementation of the ordinance, Credit Suisse's Iran Desk began to inform its Iranian Bank co-conspirator clients that neither "Order of a Customer" nor "Credit Suisse" could be used to replace references to Iranian banks on payment messages.

2291. Credit Suisse again, however, provided information about the use of the cover payment method to send USD payments, ensuring the Iranian Bank co-conspirators (and, by extension, Iran and the IRGC-QF) remained cognizant of other means of ensuring an uninterrupted flow of surreptitious USD.

2292. Although Credit Suisse's payment processing units ceased to use the "Order of a Customer" method following the Swiss Federal Banking Commission's July 2004 ordinance, Credit Suisse employees nonetheless continued removing and/or altering information in SWIFT payment order messages sent to one of its U.S. correspondent banks.

2293. For example, in May 2005, an internal Credit Suisse email stated:

If we do not have a key contact with the beneficiary's bank, we have to carry out the payment via the US, e.g. via BKTRUS33. However, no reference to Iran may

be made in the field reserved for information on the ordering party (no Iranian telephone numbers either). No such reference should be made in fields 70 or 72 either.

2294. Between March 2004 and November 2005, Credit Suisse repeatedly sent letters to its Iranian Bank co-Conspirator customers describing its internal procedures for forwarding Iranian payment orders as: “Our Payment department will stop all USD-payments initiated by your fine bank in any case and shall be effected as outlined in the drawing ‘Direct payment order and cover payment order.’”

2295. As detailed above, from August 2003 to November 2006 alone, Credit Suisse illegally processed electronic funds transfers, in the aggregate amount of at least \$480,072,032.00, through financial institutions located in the United States for the benefit of Iran and Iranian financial institutions.

2296. For a brief period of time, Credit Suisse became one of the main USD clearing and settlement banks for the Iranian banking system.

2297. In January 2006, Credit Suisse established a “Sensitive Countries” Task Force to implement the exit decision and ultimately ceased USD clearing transactions for Iran in November 2006.

2298. On September 11, 2006, Credit Suisse directed its payments centers to discontinue certain prohibited payments by an Iranian Bank Co-conspirator. Using the MT 202 cover payment method, during the six weeks from September 11, 2006 to October 27, 2006, Credit Suisse nevertheless processed 54 outbound payments involving that Iranian Bank Co-conspirator, the total value of which was in excess of \$8 million.

2299. As described herein, Credit Suisse also facilitated payments on LCs involving Mahan Air’s illegal purchase of U.S. aircraft and aircraft parts.

2300. These included the illegal purchase of an aircraft engine and an Airbus A320-232 financed by Bank Melli, Bank Refah, and Bank Sepah.

2301. In each case, Credit Suisse directed USD payments through the United States in furtherance of the Conspiracy.

2302. In March 2007, following the DPAs of Lloyds and RBS, Credit Suisse commenced an internal investigation of its historic USD funds clearing business involving U.S.-sanctioned countries and persons. Shortly thereafter, Credit Suisse was contacted by U.S. and New York law enforcement officials.

2303. On December 16, 2009, DOJ issued a press release announcing that Credit Suisse had agreed to forfeit \$536 million in USD funds to the United States and to the Manhattan District Attorney's Office in connection with violations of the IEEPA and New York State law, as a result of violations relating to transactions Credit Suisse illegally conducted on behalf of customers from, *inter alia*, Iran.

2304. In connection with a DPA that Credit Suisse entered into, DOJ filed a criminal indictment in the U.S. District Court for the District of Columbia charging Credit Suisse with one count of violating the IEEPA. Credit Suisse waived the indictment, agreed to the filing of the information, and, according to the press release, accepted and acknowledged responsibility for its criminal conduct.<sup>211</sup>

---

<sup>211</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPA, as if fully set forth herein.

2305. Credit Suisse also simultaneously entered into an agreement with OFAC to settle its violations of the IEEPA and agreed to a civil forfeiture as part of the DPA it entered into with DOJ, the Manhattan District Attorney's Office, and OFAC.<sup>212</sup>

2306. The press release announcing the agreements quoted then-Treasury Under-Secretary for Terrorism and Financial Intelligence Stuart Levey as stating “[t]his case provides a timely lesson about how Iran seeks to involve others in deceptive conduct to evade legal and regulatory controls. Those who do business with Iran expose themselves to the risk, and the consequences, of participating in transactions supporting proliferation, terrorism or sanctions evasion.”

2307. As detailed above, the DPA confirms that Credit Suisse participated and agreed to the Conspiracy detailed herein, further evidenced by the following:

- a) “Credit Suisse altered USD payment messages by: (a) removing Iranian names and references from payment messages; (b) substituting abbreviations for Iranian customer names; and (c) inserting the phrase “one of our customers” instead of the actual names of its Iranian customers. In addition, Credit Suisse, through its subsidiary Credit Suisse Asset Management Limited, United Kingdom (“CSAM”), used code words for Sanctioned Entities when executing trades involving U.S. securities that were transmitted through the U.S. Credit Suisse knew that without such alterations, amendments, and code words, automated OFAC filters at U.S. clearing banks would likely halt the payment messages and securities transactions, and, in many cases, reject or block the sanctions related transactions and report the same to OFAC. Credit Suisse manipulated payment messages and removed any identifying reference to sanctioned countries and entities so OFAC filters at the U.S. clearing banks would not identify the transactions and so that, as a result, the transactions would be automatically processed.”
- b) “In addition to altering USD payment messages, Credit Suisse instructed its Iranian customers how to format USD payments so that such payments would evade U.S. sanctions and detection by automated filters used by U.S. financial institutions. In addition, Credit Suisse promised its Iranian customers that no

---

<sup>212</sup> Pursuant to Fed. R. Civ. P. 10(c), Plaintiffs hereby adopt and incorporate by reference the DPAs and Agreements, as if fully set forth herein.

messages would leave Credit Suisse without being hand-checked by a Credit Suisse employee to ensure they had been formatted to avoid U.S. OFAC filters. When Credit Suisse employees received payment messages that were not properly formatted by Iranian clients to avoid U.S. OFAC filters, Credit Suisse would alter or amend the messages to ensure they would not be detected by U.S. financial institutions.”

- c) “In addition to training its Iranian ban customers how to format their payment messages to evade OFAC filters, Credit Suisse also gave them materials to use in training other banks on how to prepare payment messages to evade the filters.”
- d) By altering outgoing payment messages and by instructing its customers how to format messages to avoid U.S. OFAC filters, Credit Suisse caused U.S. financial institutions to process transactions that otherwise would likely have been held for investigation, rejected, or blocked, pursuant to OFAC regulations. Credit Suisse thus prevented U.S. financial institutions from filing both required BSA and OF AC-related reports with the U.S. Government. Credit Suisse continued to engage in these practices through 2006.”

2308. Credit Suisse’s settlement agreement with OFAC similarly details how Credit Suisse agreed to and participated in the Conspiracy, including the following:

- a) “For a number of years up until late 2006, Credit Suisse engaged in payment processes that prevented U.S. financial institutions from identifying the involvement of U.S. sanctions targets in funds transfers processed to and through the United States. These practices included omitting or removing information referencing sanctioned locations, entities or individuals; forwarding payment messages to U.S. financial institutions that referenced Credit Suisse as the ordering institution and that omitted the identity of the actual originating bank; filling the field on Society for Worldwide Interbank Financial Telecommunication (“SWIFT”) payment messages that indicated the originator or replacing the names of ordering customers on such payment messages with references to Credit Suisse or with phrases such as “Order of a Customer;” and using cover payments to avoid referencing parties subject to U.S. sanctions.”
- b) “With regard to Iran, Credit Suisse in Zurich engaged in similar activity in the late 1990s when, initially at the behest of its Iranian bank customers, Credit Suisse’s Iran Desk began adding internal warnings to the accounts of its Iranian bank clients, instructing Credit Suisse employees: “Do not mention the name of the Iranian bank in payment orders.” Such warnings ensured that payment orders given by the Iranian banks would not be processed automatically, but rather would be manually reviewed and effected by Credit Suisse employees. Between 2000 and 2004, the Iran Desk of Credit Suisse provided similar instructions to its Iranian bank clients via a standard letter, which stated in part: “The most important issue is that you and/or your correspondents do not mention your good

bank's name in field 52." The Iran Desk also informed Iranian bank clients that it would utilize cover payments to effect payments to or through the United States, stating, for example, "Our payment department will stop all USD payments initiated by your fine bank in any case and shall be effected [by] ... 'Direct payment order and cover payment order.'"

- c) "Teams of employees at two Credit Suisse payment centers in Zurich implemented several other methods for manually processing USD payments to or through the United States on behalf of Credit Suisse's Iranian bank clients without including references to Iran or an Iranian bank. In order to prevent straight-through processing of all payment orders sent by Iranian banks, Credit Suisse configured its payment system to interdict the payments for manual review. Credit Suisse employees then reviewed the payments to ensure they contained no references to Iran. If such references were detected, Credit Suisse employees would either delete the reference or contact the Iranian banks to request further instructions. Over time, Credit Suisse employees developed practices to omit information on the involvement of Iranian banks, including (1) entering in an empty field, or replacing the name of the Iranian banks with, "Order of a Customer" or a similar phrase instead of the ordering institution in payment messages; (2) forwarding payment messages received from Iranian banks falsely referencing "Credit Suisse" or its Bank Identifier Code instead of an Iranian bank as the originating institution; and (3) on other occasions, inserting "Credit Suisse" as the ordering institution in payments originating with an Iranian bank. In addition, Credit Suisse employees removed references to Iranian names, addresses, cities, and telephone numbers from customer payments."
- d) "In a May 2003 e-mail, a Bank Payments sector head at Credit Suisse in Zurich objected: "Today, in part, our Iranian banks send us Swift orders with CS indicated as the ordering bank in the corresponding field. --> In my opinion this must not be done, since the procedure is not in accordance with the rules, we are supporting wrong facts." [emphasis original] Shortly thereafter, in July 2003, a Credit Suisse employee, identified in documents provided to OFAC by Credit Suisse as "Executive 4," requested that an employee from the European Banking Federation anonymously inquire from OFAC the conditions under which payments from Iran into the United States were permitted. The European Banking Federation's employee replied to Executive 4 by email on July 24, 2003, that":
  - i. "The traznsaction [sic] must go through a non-US and a non-Iranian off-shore correspondent bank (which is the case in your situation);"
  - ii. "The citizen beneficiary of the money in the US will have to provide an affidavit to US bank mentioning that the money is for pure personal use (no commercial or other purpose)."
- e) "Executive 4 then requested that the head of the Iran Desk ask a Customer Payments team leader to analyze the characteristics of the payments from Iran into

the United States that were processed by Credit Suisse in June 2003. On July 30, 2003, the head of the Iran Desk reported back to Executive 4: ‘The volume is rather considerable... The average amount... does not quite correspond to the criteria of small private payments.’”

- f) “In August 2003, Credit Suisse reached an agreement with the London branches of a number of Iranian banks to take over their USD clearing activity, As a result of this agreement, Credit Suisse became one of the main USD clearing banks for the Iranian banking system. In or around March 2004, the risk committee of the Credit Suisse Group board conducted a review of the procedures Credit Suisse had in place to prevent OFAC violations. The practice of ensuring that USD payments did not identify the Iranian origin continued after that point.”
- g) “In July 2004, an ordinance issued by the Swiss Federal Banking Commission on money laundering to implement the Financial action Task Force’s Special Recommendation on Terrorist Financing VII entered into force. The ordinance required the disclosure of the remitter in payment orders, and prompted Credit Suisse to issue an internal directive prohibiting the use of the “Order of a Customer” method when making international wire transfers. In preparation for the implementation of the ordinance, in April 2004 Credit Suisse’s Iran Desk began to inform its Iranian bank clients that neither “Order of a Customer” nor “Credit Suisse” could be used to replace references to Iranian banks on payment messages. Credit Suisse again provided information about the use of the cover payment method to send USD payments. Although Credit Suisse’s payment processing units ceased completely the use of the “Order of a Customer” method following the issuance of the Swiss Federal Banking Commission ordinance, other practices persisted in which Credit Suisse employees removed or altered information in SWIFT payment messages sent to a U.S. correspondent bank.”
- h) “Specifically, from on or about August 19, 2003, to on or about November 1, 2006, Credit Suisse processed 4,775 electronic funds transfers, in the aggregate amount of USD 480,072,032.00, through financial institutions located in the United States to the benefit of the Government of Iran and/or persons in Iran, including various Iranian financial institutions, in apparent violation of the prohibition against the “exportation, ... directly or indirectly, from the United States, ... of any ... services to Iran or the Government of Iran,” 31 C.F.R. § 560.204.”
- i) “The apparent violations by Credit Suisse described above provided substantial economic benefit to Iran, Burma, Sudan, Cuba, Libya, and a person designated pursuant to E.O. 13348, thereby undermining the U.S. national security, foreign policy, and other objectives of the related sanctions programs.”

2309. Based on the conduct described above, Credit Suisse entered into DPA with the DOJ and with the District Attorney of the County of New York based on Credit Suisse’s

violation of New York and U.S. law. In conjunction with reaching these agreements, Credit Suisse agreed the following facts are true and correct:

- a) Beginning in the mid-1990s and continuing through 2006, Credit Suisse systematically and knowingly moved hundreds of millions of dollars illegally through the U.S. financial system, including through its own bank branches and through various correspondent banks, to certain countries and entities identified by the United States as state sponsors of terrorism, including Iran, by:
  - i. removing or falsifying references from outgoing USD payment messages that involved countries, banks, or persons listed as parties or jurisdictions sanctioned by OFAC (collectively, “the Sanctioned Entities”);
  - ii. advising the Sanctioned Entities how to evade automated filters at U.S. financial institutions primarily located in New York, New York; and
  - iii. causing U.S. financial institutions to unknowingly process sanctioned transactions.
- b) By engaging in this conduct, Credit Suisse:
  - i. deceived U.S. financial institutions into processing transactions they would not otherwise have processed;
  - ii. prevented U.S. financial institutions from filing required Bank Secrecy Act and OFAC-related reports with the U.S. government;
  - iii. caused false information to be recorded in the records of U.S. financial institutions; and
  - iv. caused U.S. financial institutions not to make records they otherwise would have been required by U. S. law to make.
- c) Specifically, as part of its business transactions in the United States, Credit Suisse altered USD payment messages to prevent OFAC filters at U.S. clearing banks from identifying the transactions as Iranian transactions and so that, as a result, the transactions would be automatically processed. It did this by:
  - i. removing Iranian names and references from payment messages;
  - ii. substituting abbreviations for Iranian customer names;
  - iii. inserting the phrase “one of our customers” instead of the actual names of its Iranian customers; and

- iv. having one of its subsidiaries in the United Kingdom use code words for Sanctioned Entities when executing trades involving U.S. securities transmitted through the United States.
- d) Further, Credit Suisse instructed its Iranian customers how to format USD payments so that those payments would evade U.S. sanctions and detection by automated filters used by U.S. financial institutions.
- e) Further, Credit Suisse promised its Iranian customers that no payment messages would leave Credit Suisse without being hand-checked by a Credit Suisse employee to ensure they had been formatted to avoid U.S. OFAC filters; when Credit Suisse employees received payment messages that were not properly formatted by Iranian clients to avoid U.S. OFAC filters, Credit Suisse would alter or amend the messages to ensure they would not be detected by U.S. financial institutions.
- f) To further its scheme to evade U.S. sanctions and detection by automated filters used by U.S. financial institutions, Credit Suisse also gave its Iranian bank customers materials to use in training other banks on how to prepare payment messages to evade the U.S. OFAC filters.
- g) By altering outgoing payment messages and by instructing its Iranian customers how to format messages to avoid U.S. OFAC filters, Credit Suisse caused U.S. financial institutions to process transactions that otherwise would likely have been held for investigation, rejected, or blocked, pursuant to U.S. OFAC regulations. Credit Suisse thus prevented U.S. financial institutions from filing both required BSA and OFAC-related reports with the U.S. Government. Defendants Credit Suisse continued to transact business in the United States using these practices through 2006.

2310. Credit Suisse also engaged in processing illegal USD transactions on behalf of Iranian entities through a correspondent bank in the United States.

2311. According to the CHIPS-NY website, Credit Suisse used the following U.S. financial institutions in New York to clear and settle U.S. Eurodollar transactions:

- a) Defendants HSBC Bank USA, N.A. (identified by CHIPS-NY participant number 0108 and Fedwire routing number 021001088);
- b) The Bank of New York Mellon (identified by CHIPS-NY participant number 0001 and Fedwire routing number 011001234);
- c) Deutsche Bank Trust Co Americas (identified by CHIPS-NY participant number 0103 and Fedwire routing number 021001033); and

- d) Wells Fargo Bank NY International (identified by CHIPS-NY participant number 0509 and Fedwire routing number 026005092).

2312. Based on this and other illegal conduct on behalf of Iran aimed at the United States financial system, Credit Suisse chose to enter into sweeping DPAs, admitting that its conduct violated New York State and United States laws, specifically the IEEPA, Title 50, United States Code § 1705, to wit, Title 31, C.F.R., Sections 560.203 and 560.204, that prohibit: (a) the exportation of a service to Iran from the United States without authorization; and (b) any transaction within the United States that evaded and avoided, or had the purpose of evading and avoiding such regulations. Credit Suisse admits that its conduct violated United States federal law. Credit Suisse further admitted that its conduct violated New York state law (Penal Law §§ 175.05 and 175.10).

2313. The DPAs required the ongoing submission to the jurisdiction of the United States for purpose of trying to remediate the illegal actions taken on behalf of Iran and others, and to prevent such actions from happening in the future. To that end, Credit Suisse agreed:

- a) To pay to the United States \$268,000,000, and pay a separate and additional amount of \$268,000,000 to the State of New York;
- b) To waive any challenges to the venue or jurisdiction of the United States District Court for the District of Columbia;
- c) To work in conjunction with the DOJ, United States financial regulation bodies, and the District Attorney's office for New York, to ensure compliance with a host of matters required by a DPA entered into by Credit Suisse and federal and New York officials in December 2009;
- d) To accept and acknowledge responsibility for its conduct and that of its employees;
- e) To a continuing relationship with the DOJ and the District Attorney of New York to ensure Credit Suisse no longer tried to circumvent United States law for the purpose of laundering money on behalf of sanctioned entities, including Iran, or face prosecution in the United States;

- f) To conduct in-depth training of Credit Suisse employees, and certify to the United States that such training had been completed;
- g) To certify that Credit Suisse has written policies to require proper payment messaging;
- h) To maintain certain transaction documentation;
- i) To abide by orders and regulations of the Board of Governors of the Federal Reserve System;
- j) To demonstrate its future good conduct and full compliance with FATF international AML and Combating Financing of Terrorism best practices and the Wolfsberg AML Principles for Correspondent Banking;
- k) To retain and provide to the United States relevant documents, electronic data, or other objects in Credit Suisse's possession, custody, or control relating to the relevant transactions;
- l) To be prosecuted for the crimes charged if it were to materially breach the substance of the agreement reached with the United States;
- m) To not make any public statement contradicting, excusing or justifying the conduct it admitted to in the DPA; and
- n) To include in any sales agreements for any of its operations involved in the transmission of USD a requirement the purchasing entity be bound by the terms and conditions of the DPA.

**C. DEFENDANT BANK SADERAT'S AND IRANIAN BANK Co-CONSPIRATORS' AGREEMENT TO, AND PARTICIPATION IN, THE CONSPIRACY**

2314. On September 8, 2006, OFAC amended § 560.516 of the ITRs and excluded Defendant Bank Saderat from the Iranian U-turn exemption.

2315. In announcing the 2006 change to the ITRs excluding Bank Saderat from the U-turn exemption, OFAC stated:

OFAC has amended the Iranian Transactions Regulations [] to cut off Bank Saderat, one of Iran's largest government-owned banks, from the U.S. financial system. Bank Saderat has been a significant facilitator of Hezbollah's financial activities and has served as a conduit between the Government of Iran and Hezbollah....

2316. According to then-Under Secretary for Terrorism and Financial Intelligence Stuart Levey, “Bank Saderat facilitates Iran’s transfer of hundreds of millions of dollars to Hezbollah and other terrorist organizations each year. We will no longer allow a bank like Saderat to do business in the American financial system, even indirectly.”

2317. The Treasury Department press release announcing the changes to the Iranian Transactions Regulations stated that “a Hezbollah-controlled organization [] has received \$50 million directly from Iran through Bank Saderat since 2001.”

2318. Assistant Secretary for Terrorist Financing and Financial Crimes Daniel Glaser testified before the Senate Committee on Banking, Housing and Urban Affairs that “Hezbollah uses Saderat to send money to other terrorist organizations as well.”

2319. For many years preceding the revocation of its U-turn exemption, Bank Saderat illegally routed its USD transactions through the United States with the assistance of various Western commercial banks, including Defendants herein.

2320. From 2002 forward, Defendant Bank Saderat continued its existing practice of: (1) illegally routing its USD transactions through the United States; and (2) transferring tens of millions of dollars to Hezbollah and other designated terrorist groups.

2321. Notwithstanding the revocation of its access to the Iranian U-turn exemption, Defendant Bank Saderat continued to illegally direct USD transactions through the United States with the active assistance of Defendants listed herein.

2322. On February 13, 2004, Defendants SCB opened accounts for Defendant Bank Saderat. It also maintained other accounts for Bank Saderat Iran, including an account at SCB, Dubai.

2323. During the Relevant Period, and as described in more detail below, Defendant Bank Saderat, working in concert with SCB, financed the illegal acquisition of various U.S.-origin export-controlled goods on behalf of Mahan Air and various sub-agencies of MODAFL.

2324. For example, SCB facilitated at least 10 transactions involving LCs valued at \$1,559,127, which involved the shipment of U.S.-origin export-controlled aircraft parts sold by the Singapore-based Monarch Aviation, a company that was part of Iran's illegal procurement network, to various MODAFL sub-agencies.

2325. A sub-agency of MODAFL obtained a LC issued by Bank Refah, Iran, and sent it to SCB's branch in Singapore (where the Iranian front company Monarch Aviation maintained accounts) while reimbursement authorization was sent to the Iran Overseas Investment Bank London, *i.e.* Defendant Bank Saderat's predecessor, which in turn either directly financed the illegal acquisition of goods from the United States, or provided a surety for Bank Refah's payment.<sup>213</sup>

2326. The goods were shipped by Iran Air<sup>214</sup> from Kuala Lumpur Airport, Malaysia to Tehran Airport, Iran.

2327. The LCs were refinanced by SCB's Dubai branch through its credit facility with the CBI, with payment being made to Monarch Aviation's account with SCB Singapore through

---

<sup>213</sup> The Reimbursing Bank usually pays the Negotiating Bank (in this case SCB) against a valid reimbursement authority received from the Issuing Bank (in this case Bank Refah) and a validated statement from the Negotiating Bank that the documents complied with LC terms, but in certain cases it only serves as a surety for the payment. SCB-London was also one of Bank Refah's correspondent banks in the UK.

<sup>214</sup> "Iran's national airline carrier, Iran Air, is a commercial airline used by the IRGC and Iran's Ministry of Defense and Armed Forces Logistics (MODAFL) to transport military related equipment.... Iran Air has provided support and services to MODAFL and the IRGC through the transport and/or transfer of goods for, or on behalf of, these entities. On numerous occasions since 2000, Iran Air shipped military-related electronic parts and mechanical equipment on behalf of MODAFL." See <https://www.treasury.gov/press-center/press-releases/Pages/tg1217.aspx>.

the latter's USD account with SCB London, which in turn received the funds into its USD nostro account with SCB's New York branch.

2328. In another instance discussed infra, Defendant Bank Saderat knowingly sent a concealed and illegal payment via SCB's New York branch and JP Morgan Chase, New York, to SCB Dubai on behalf of a MODAFL's subsidiary, the IHSRC.

2329. The payment facilitated IHSRC's acquisition (via a company named Jetpower) of U.S. manufactured helicopter parts through an elaborate money laundering scheme intended to conceal from U.S. authorities: (1) the unlawful acquisition of U.S.- manufactured equipment for Iran's military; (2) the complex layering of the transaction involving Bank Mellî's branches in London and Hong Kong; and (3) Bank Refah and Defendant Bank Saderat's involvement with SCB.

2330. The HSBC Defendants also maintained one or more accounts for Defendant Bank Saderat during the Relevant Period.

2331. In an October 9, 2006 email, Defendants HBME's Regional Head of Legal and Compliance noted the U.S. government's "direct evidence against [Defendants] Bank Saderat particularly in relation to the alleged funding of Hezbollah" but nonetheless maintained the account(s) thereafter and continued to facilitate transactions for Bank Saderat Plc.

2332. As noted *supra*, in October 2007, Bank Saderat Iran (including Defendant Bank Saderat), was designated an SDGT pursuant to E.O. 13224.

2333. The U.S. Treasury Department's press release regarding Bank Saderat's designation stated:

Bank Saderat, its branches, and subsidiaries: Bank Saderat, which has approximately 3200 branch offices, has been used by the Government of Iran to channel funds to terrorist organizations, including Hezbollah and E.U.-designated terrorist groups Hamas, PFLP-GC, and Palestinian Islamic Jihad. For example,

from 2001 to 2006, Bank Saderat transferred \$50 million from the Central Bank of Iran through its subsidiary in London to its branch in Beirut for the benefit of Hezbollah fronts in Lebanon that support acts of violence.

2334. As set forth below, Defendants Barclays closed its accounts for Defendant Bank Saderat, in 2008, months after Defendant Bank Saderat was designated an SDGT, and more than a year after the U.S. Treasury Department reported that “[Defendants] Bank Saderat facilitates Iran’s transfer of hundreds of millions of dollars to Hezbollah and other terrorist organizations each year.”

2335. The HSBC Defendants, and Defendants Commerzbank, SCB, Barclays, and Credit Suisse altered, falsified, or omitted information from Eurodollar payment order messages they facilitated on behalf of Bank Saderat (and Defendant Bank Saderat) at all times knowing, or deliberately indifferent to the fact, that Bank Saderat was facilitating Iranian-sponsored terrorism and, after October 2007, knowing, or deliberately indifferent to the fact, that Bank Saderat (including Defendant Bank Saderat) was an SDGT so-designated for its very role as a “significant facilitator of Hezbollah’s financial activities and has served as a conduit between the Government of Iran and Hezbollah.”

2336. Moreover, as a Lebanese-based terrorist organization, Hezbollah was (and remains) particularly in need of USD funds because much of the Lebanese economy is primarily conducted using USD funds.

2337. Accordingly, Defendant Bank Saderat’s provision of tens of millions of dollars to Hezbollah provided Hezbollah with substantial assistance in carrying out its terrorist activities in Iraq, including Hezbollah’s participation in the terrorist attacks that killed and injured the Plaintiffs.

2338. Moreover, Plaintiffs' deaths and injuries herein were a reasonably foreseeable result of Defendant Bank Saderat's provision of tens of millions of dollars to Hezbollah.

2339. Throughout the Relevant Period, the CBI maintained accounts at Bank Melli Iran, Bank Melli Plc, Bank Saderat Iran and Defendant Bank Saderat in various currencies, including USD.

2340. The CBI/Markazi is fully controlled and run by individuals directly appointed by the Government of Iran.

2341. At all relevant times, the CBI has not functioned in the same manner as central banks in Western countries that are institutionally designed to be independent from political interference, nor is its purpose limited to "regulating" Iranian banks and managing Iran's currency and internal interest rates.

2342. Instead, the CBI is an alter-ego and instrumentality of Iran and its Supreme Leader, and it has routinely used Iranian banks like Bank Melli Iran and Bank Saderat Iran as conduits for terror financing and weapons proliferation on behalf of the Iranian regime.

2343. At all relevant times, the CBI was an active participant in the Conspiracy. For example, leading up to the adoption of UN Security Council Resolution 1747 (March 2007), which resulted in the freezing of assets belonging to Iran's Bank Sepah, the CBI furthered the Conspiracy by using non-Iranian financial institutions to shield Bank Sepah's assets from the impact of impending sanctions.

2344. Bank Melli Iran's U.K. subsidiary (later Bank Melli Plc) managed the CBI's accounts in Europe.

2345. In the wake of U.S. and later European Union designations against Iranian banks (including Bank Saderat and Bank Melli), the CBI often acted as a secret proxy for those designated entities.

2346. As part of the Conspiracy, the CBI utilized Defendant Bank Saderat to transfer USD funds to Hezbollah.

2347. The CBI also maintained accounts, and unlawfully transferred USD funds in furtherance of the Conspiracy, with the assistance of Defendants SCB, Royal Bank of Scotland N.V., and the HSBC Defendants, including facilitating billions of dollars in USD funds transfers on behalf of the IRGC, through the NIOC, which was designated as an SDN by the United States because it was an IRGC agent during the Relevant Period.

2348. As such, illicit transfers on behalf of the NIOC at that time were not for the benefit of a legitimate agency, operation or program of Iran. The Superseding Indictment filed in *U.S. v. Zarbab* (filed in the S.D.N.Y. (1:15-cr-00867)) demonstrates that NIOC continued to participate in the Conspiracy and launder USD through U.S. financial institutions in 2013.

2349. In addition, the Iran Threat Reduction and Syria Human Rights Act 2012<sup>215</sup> stated that:

It is the sense of Congress that the National Iranian Oil Company and the National Iranian Tanker Company are not only owned and controlled by the Government of Iran but that those companies provide significant support to Iran's Revolutionary Guard Corps and its affiliates.

2350. Moreover, according to a published report, the NIOC even took an active role in support of Iran's terrorist activities in Iraq by providing intelligence in support of attacks against

---

<sup>215</sup> See [https://www.treasury.gov/resource-center/sanctions/Documents/hr\\_1905\\_pl\\_112\\_158.pdf](https://www.treasury.gov/resource-center/sanctions/Documents/hr_1905_pl_112_158.pdf).

Coalition Forces along the Iranian border by using its own helicopters to conduct surveillance on Coalition Forces' FOBs.

2351. In early 2001, and in furtherance of the Conspiracy, the CBI asked Defendants SCB to act as its correspondent bank with respect to payments on behalf of the NIOC.

2352. As alleged herein, SCB agreed to participate in the Conspiracy and remove identifying data on SWIFT-NET messages for these and other wire transfers.

2353. Thereafter, between 2001 and 2006, the CBI sent approximately 2,226 payment order messages for a total value of \$28.9 billion to SCB London, the vast majority of which were illegally routed through the U.S. as described herein.

2354. During the same time period, the CBI also maintained a Eurodollar credit facility at SCB's branch in Dubai, UAE, which it used to assist Iran in illegally acquiring technology and components on behalf of MODAFL.

2355. As detailed further below, and in furtherance of the Conspiracy, the CBI and Defendants RBS (which also maintained Eurodollar accounts for the CBI, and had numerous financial and business dealings with the CBI) conspired to provide illegal material support to Iran and Iranian parties.

2356. Between 2002 and 2004, Defendants RBS accepted USD Eurodollar deposits from the CBI on a regular basis with an average deposit size in the range of \$200 million USD, and the CBI instructed, and RBS agreed, to follow illegal procedures to launder USD-denominated Eurodollar deposits to the CBI's Eurodollar and local currency accounts with other European banks with branches or offices in London.

2357. In furtherance of the Conspiracy, the CBI coordinated with Defendants RBS's Central Bank Desk in Amsterdam regarding the procedure to be followed for repayment of USD deposits to their Eurodollar accounts with European banks with offices or branches in London.

2358. This procedure stipulated that payment order messages sent to U.S. clearing banks for payment of USD funds to the CBI should not contain any reference to the Central Bank of Iran, or any other reference relating to Iran.

2359. In 2001, the CBI also approached members of the HSBC Group, specifically Defendants HBME and HSBC-London, to obtain their agreement to move the CBI's clearing and settlement business from National Westminster Bank Plc to the HSBC Defendants, and intended to clear USD funds transactions through Defendants HSBC-US.

2360. Pursuant to that agreement, the CBI eventually moved its Eurodollar accounts to the HSBC Defendants, and by late 2003, the CBI was one of six Iranian banks that used members of the HSBC Group for (mostly illegal) correspondent banking through the USD clearing and settlement in New York.

2361. With Defendants HSBC Holdings' knowledge, and in furtherance of the Conspiracy, Defendants HBME and HSBC-London manually intervened in the processing of payment orders by the CBI by removing: the Central Bank of Iran's name; its SWIFT-NET account (identified by BIC address BMJIIRTH); and country of origin (Iran).

2362. Defendants HSBC-US also knew that other HSBC Defendants were altering and omitting information in SWIFT-NET payment order messages regarding Iranian parties, i.e. "stripping" these transactions, but nevertheless knowingly continued processing transactions despite that very knowledge.

2363. Bank Melli Iran, one of the largest banks in Iran, was established in 1927 by order of the Iranian Parliament.

2364. Following the Iranian Revolution in 1979, all banks in Iran were nationalized, and even today most are effectively controlled by the Iranian regime.

2365. Melli Bank Plc in London, England, was established in January 2002 as a wholly-owned subsidiary of Bank Melli Iran.

2366. According to the U.S. government, from 2004 to 2011, Bank Melli Iran and Melli Bank Plc in London transferred approximately \$100 million USD to the IRGC-QF, which trained, armed, and funded terrorist groups that targeted, killed and maimed American and Iraqi forces and civilians.

2367. Specifically, according to the U.S. government in a November 10, 2009 diplomatic cable:

[The] Islamic Revolutionary Guards Corps (IRGC) and IRGC-Qods Force, who channel funds to militant groups that target and kill Coalition and Iraqi forces and innocent Iraqi civilians, have used Bank Melli and other Iranian banks to move funds internationally. Bank Melli used deceptive banking practices to obscure its involvement from the international banking system by requesting that its name be removed from financial transactions when handling financial transactions on behalf of the IRGC.

2368. Bank Melli Iran and Melli Bank Plc were designated as SDNs pursuant to E.O. 13382 in October 2007, and included on OFAC's SDN list, which resulted in, inter alia, their exclusion from the U-turn exemption for Iranian Eurodollar transactions.

2369. The U.S. Treasury Department press release announcing the designation stated:

Bank Melli also provides banking services to the [Iranian Revolutionary Guard Corps] and the Qods Force. Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least \$100 million to the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking

system. For example, Bank Melli has requested that its name be removed from financial transactions.

2370. In April 2008, Assistant Treasury Secretary for Terrorist Financing Daniel Glaser testified before the House Committee on Foreign Affairs, Subcommittee on the Middle East and South Asia and the Subcommittee on Terrorism, Nonproliferation and Trade, confirmed that:

Entities owned or controlled by the IRGC or the Qods Force use Bank Melli for a variety of financial services. From 2002 to 2006, Bank Melli was used to send at least \$100 million to the Qods Force. When handling financial transactions on behalf of the IRGC, Bank Melli has employed deceptive banking practices to obscure its involvement from the international banking system. For example, Bank Melli has requested that its name be removed from financial transactions.

2371. In mid-2007, Bank Melli-Hamburg transferred funds for the DIO.

2372. DIO is an Iranian government-owned defense manufacturer whose name, logo and/or product tracking information was stamped on munitions found in weapons caches that were seized from the Special Groups in Iraq; including large quantities of weapons produced by DIO in 2006 and 2007 (for example, 107 millimeter artillery rockets, as well as rounds and fuses for 60 millimeter and 81 millimeter mortars.).

2373. Since at least the mid-1980s, Bank Melli has maintained accounts, at one time or another, with Defendants RBS, Barclays, Credit Suisse, SCB, Commerzbank, and the HSBC Defendants.

2374. As early as 1987, Bank Melli instructed Defendants Barclays to process transactions in favor of Bank Melli's London branch by referencing only Bank Melli's account number at Midland Bank Plc in London without referencing Bank Melli Iran's name in the SWIFT-NET payment orders.

2375. Bank Melli further instructed Barclays to send separate payment order message instructions, which included full transaction details, to Bank Melli's London Branch.

2376. Barclays agreed and assisted Bank Melli in its illegal conduct and continued to do so even after Bank Melli was designated by the United States and publicly identified as a major source of the IRGC's funding.

2377. No later than December 2000, Bank Melli opened a Eurodollar account with Defendants RBS's branch in Dubai, UAE and worked with RBS to strip its USD-denominated transactions.

2378. Similarly, in July 2003, Defendants SCB learned that a competitor was exiting the Iranian business completely and sought to pick up this business and add Eurodollar accounts for five Iranian banks at SCB-London. Bank Melli was among the banks whose business SCB expressly sought to (and did) acquire.

2379. In January 2004, SCB decided to proceed with the Iranian business, and no later than February 13, 2004, SCB opened Eurodollar accounts for Bank Melli and thereafter participated in the Conspiracy by facilitating unlawful transactions for Bank Melli.

2380. In addition, Bank Melli Iran's branch in the UAE was instrumental in facilitating U.S. sanctions-evading trade-finance and Eurodollar payment transactions on behalf of Mahan Air and MODAFL.

2381. For example, Bank Melli issued a LC to Mahan Air in August 2004 through SCB Dubai in favor of a UAE-based company called Aeronautical & Security for the shipment of an aircraft engine (identified by model number CF6-50C2) manufactured by General Electric and shipped from Luxemburg to Tehran, Iran.

2382. Bank Melli UAE instructed Credit Suisse, Zurich to make the payment, which in turn instructed Bank of New York in New York (one of Credit Suisse's U.S. clearing and

settlement banks) to credit SCB's New York branch for further credit to the account of SCB Dubai, which then credited Aeronautical & Security's Eurodollar account.

2383. In another example, Bank Refah Kargaran, Iran issued a LC in USD to a MODAFL sub-agency through SCB Dubai in favor of a Dubai-based company called FP Aeroparts for the illegal shipment (via Iran Air) of U.S. aircraft parts.

2384. Bank Melli served as the Reimbursing Bank on the trade-finance transaction, and it subsequently instructed Credit Suisse, Zurich to debit its Eurodollar account as part of the flow of USD funds between the LCs counterparties.

2385. As the LC transaction proceeded, Credit Suisse then further instructed The Bank of New York to pay SCB's New York branch (the clearing bank for the transaction), which further credited the USD account it maintained for SCB, Dubai with the amount due for the shipment of aircraft parts.

2386. To close-out the LC transaction, SCB, Dubai then credited the Eurodollar account it maintained on behalf of FP Aeroparts Middle East for the amount of the shipment.

2387. During the Relevant Period, Defendants Credit Suisse maintained Eurodollar accounts in Zurich, Switzerland on behalf of Bank Melli.

2388. Credit Suisse also instructed and trained Bank Melli employees, and conspired with Bank Melli, on ways to format Bank Melli's payment orders so the resulting SWIFT-NET messages would avoid detection by the automated filter algorithms in U.S. depository institutions' automated OFAC sanction screening software.

2389. During the Relevant Period (and beginning no later than July 2003), Defendants Commerzbank also conspired with Bank Melli to route its Eurodollar clearing and settlement

business through Commerzbank's correspondent banking relationships and SWIFT-NET accounts.

2390. Commerzbank further advised Bank Melli to list “non ref” in the ordering party field in all payment order messages because it would trigger a manual review of the overall Eurodollar payment transaction, thereby enabling Commerzbank personnel to ensure the SWIFT-NET messages did not contain any information linked to Iran.

2391. Defendants HSBC-London also maintained Eurodollar accounts for Bank Melli Iran, and it used HSBC-US to provide illegal USD funds clearing and settlement services for Bank Melli during the Relevant Period.

2392. Yet despite the fact several SWIFT-NET payment order messages were supposed to have been fully “stripped” by HSBC-London—before their transmittal to the U.S.—they were nevertheless blocked by the HSBC-US OFAC filter in New York because Bank Melli was referenced in error (thus placing HSBC-US on notice that HSBC-London was working in concert with Bank Melli to evade U.S. law, regulations and economic sanctions against Iran).

2393. Even with these blatant warning signs, HSBC-US continued to routinely provide Eurodollar clearing and settlement services to the HSBC Defendants, knowing full well they were violating U.S. laws and regulations by laundering money on behalf of Bank Melli.

2394. Because, as discussed below, HSBC-US knew of this unlawful conduct—and continued to facilitate it—HSBC-US violated, *inter alia*, 18 U.S.C. § 2332d.

**D. DEFENDANTS KNOWINGLY PROVIDED IRAN WITH U.S. DOLLARS, THEREBY ALLOWING IRAN TO FUND THE TERRORIST ATTACKS THAT KILLED OR INJURED PLAINTIFFS**

2395. As detailed above, Defendants provided sanctioned Iranian entities with significant access to the U.S. financial system—allowing Iran to launder billions of USD to fund its terrorist campaign. They did so knowing Iran was a State Sponsor of Terrorism and needed

access to USD to finance its terror campaign. Further, they did so knowing Iran would use the USD funds for terrorist attacks, including those Terrorist Attacks perpetrated against Plaintiffs.

2396. Defendants did more than simply maintain a bank account and receive or transfer funds. As part of the Conspiracy, Defendants funneled billions of USD to Iran—money without which Iran could not fund its terrorist activities—knowing that such funds were being directed to Iran who was then directing those very same funds to Iranian Agents and Proxies, and that such funds were being used to perpetrate acts of international terrorism, including the Terrorist Attacks which killed, maimed, or otherwise injured Plaintiffs and/or their family members.

2397. Defendants knew the entities to which they provided services are/were engaged in terrorist activities, and thus, providing USD to those entities constitutes material support.

2398. At the time Defendants provided the material support identified herein to the Terrorist Groups responsible for the Terror Attacks, Defendants knew that monies provided to such Terrorist Groups would be used in the commission of terrorist acts. Thus, Defendants collected funds “with the intention that such funds be used or with the knowledge that such funds were to be used for terrorist purposes.”<sup>216</sup>

2399. Because money is fungible, giving support intended to aid an organization’s non-terroristic activities frees up resources that can be used for terrorist acts. Such is the case here. To the extent the organizations that received funds from Defendants used such funds for non-terroristic purposes, these funds freed up resources that could be used by those organizations for terrorist acts.

2400. In doing so, Defendants agreed to the essence of the Conspiracy.

---

<sup>216</sup> 18 U.S.C. § 2339C.

### **VIII. THE ACTS OF DEFENDANTS CAUSED PLAINTIFFS' INJURIES AND DEATHS**

2401. As discussed herein, Iran has a long history of materially supporting the Terrorist Groups. Simply put, Iran is no stranger to supporting terrorist attacks perpetrated by FTOs and other terrorist organizations against U.S. nationals with the intent to terrorize, kill or cause severe bodily and emotional harm.

2402. Here, Iran and/or its Agents and Proxies used U.S. currency knowingly provided to them by Defendants to fund the very Terrorist Groups who perpetrated the Terrorist Attacks which killed or injured Plaintiffs.

2403. Without the material support provided by Defendants to Iran and its Agents and Proxies, the Terrorist Groups would not have been able to carry out such Terrorist Attacks on the scale and with the lethality in which they were perpetrated.

2404. Moreover, it is entirely foreseeable that the material support would enable and facilitate attacks on innocent persons, including Plaintiffs, in areas known to be occupied by U.S. citizens, and would cause injury or death to persons who are citizens of the United States.

2405. At all relevant times, Defendants knew or were deliberately indifferent to the fact they were unlawfully conducting business with Agents and Proxies of Iran. Thus, Defendants knew they were directly involved with Iran and its Agents and Proxies—entities Defendants knew, or were recklessly indifferent to the fact that they, were engaged in terrorist activities and that such terrorist activities were aimed at U.S. nationals, including Plaintiffs. Because all terrorist activities carry the foreseeable risk of killing or injuring innocent persons, including Plaintiffs, Defendants conduct as set forth herein was a proximate cause of Plaintiffs' deaths and injuries.

2406. Because Defendants entered into and fully participated in the Conspiracy, and because the Conspiracy could not have been effectuated without Defendants' assistance and participation, Defendants caused Plaintiffs' injuries and deaths.

2407. Further, through the Conspiracy, Defendants provided financial services and material support, and aided and abetted Iran and its Agents and Proxies, including the Terrorist Groups responsible for the Terrorist Attacks.

## **IX. CLAIMS FOR RELIEF**

### **A. FIRST CLAIM FOR RELIEF: PRIMARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST ALL DEFENDANTS FOR PROVIDING MATERIAL SUPPORT TO TERRORIST GROUPS IN VIOLATION OF 18 U.S.C. § 2339A**

2408. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2409. Defendants provided material support to Iran, its Agents and Proxies, and the Terrorist Groups.

2410. By providing material support or resources, or concealing or disguising the nature, location, source, or ownership of material support or resources, to terrorists, knowing or intending that such material support be used in preparation for, or in carrying out, a violation of any offense set forth in 18 U.S.C. §§ 32, 37, 81, 175, 229, 351, 831, 842(m) or (n), 844(f) or (i), 930(c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155, 2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, and/or 2442, 42 U.S.C. § 2284, 49 U.S.C. §§ 46502 or 60123(b), and/or any offense listed in 18 U.S.C. § 2332b(g)(5)(B), each Defendant committed acts of international terrorism and is liable for damages to each Plaintiff pursuant to 18 U.S.C. § 2333(a).

2411. Each Defendant also provided material support, in the form of U.S. currency and financial services and financial securities, by knowingly facilitating the transfer of hundreds of

billions of USDs and by underwriting billions of USDs in trade finance transactions. Congress defined “Material support or resources” in 18 U.S.C. § 2339A to include “...any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, . . .”<sup>217</sup> Defendants provided such material support by, among other things, knowingly facilitating the transfer of hundreds of billions of USDs to known terrorist organizations (including the Terrorist Groups, or to known front companies for such terrorist organizations, including the NIOC, Mahan Air, Iran Air, Khatam-al Anbiya Construction, IRISL (and multiple IRISL entities), Bank Melli (including Bank Melli plc), Bank Saderat (including Bank Saderat plc), Bank Mellat, Bank Sepah, and Bank Markazi, using Defendants’ USD clearing services, as well as the underwriting billions of USDs in trade finance transactions. Such conduct is squarely within the definition of “material support or resources” contemplated by Congress when enacting 18 U.S.C. § 2339A, and violates Congress’ stated goal of cutting off the flow of money to terrorists.

2412. Each Defendant also provided material support in the form of expert advice and assistance to Iran and its Agents and Proxies, specifically including the Terrorist Groups. Included in the definition of “Material support or resources” is “expert advice or assistance.” Congress defined “expert advice or assistance” in 18 U.S.C. § 2339A to include “advice or assistance derived from ...technical or other specialized knowledge.”<sup>218</sup>

---

<sup>217</sup> 18 U.S.C. § 2339A(b).

<sup>218</sup> *Id.*

2413. Defendants each received extensive guidance and training on detecting and preventing the flow of money to terrorists from the government agencies tasked with enforcing the laws, knowing or with deliberate indifference to the fact Iran would use that specialized and highly technical knowledge to illegally transfer billions of USD to Iran and its Agents and Proxies without detection by the various enforcement agencies, Defendants brazenly provided that technical and highly specialized knowledge to Iran and its Agents and Proxies as part of their package of illicit financial services.

2414. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant also had knowledge of the Iran's Agents' and Proxies' connection to terrorism, in general, and to the massive waves of terrorist attacks targeting, killing, and injuring U.S. nationals in Iraq.

2415. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew, or was deliberately indifferent to the fact, that Hezbollah was designated an FTO, SDT and SDGT.

2416. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew, or was deliberately indifferent to the fact, that al Qaeda was designated an FTO.

2417. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew, or was deliberately indifferent to the fact, that AAI was designated an FTO.

2418. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew, or was deliberately indifferent to the fact, the IRGC-QF was designated an SDGT.

2419. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew, or was deliberately indifferent to the fact, that Bank Saderat (including Defendant Bank Saderat) was designated an SDGT.

2420. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew, or was deliberately indifferent to the fact, the IRGC was designated an SDN.

2421. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant knew or was deliberately indifferent to the fact Bank Melli (including Melli Bank Plc), Bank Saderat (including Defendant Bank Saderat), Bank Mellat, Bank Sepah, and KAA were designated SDNs before November 2008, and, as such, were excluded from accessing the U-Turn exemption in the Iranian Transaction Regulations.

2422. At the time each Defendant provided material support to Iran's Agents and Proxies each Defendant also knew or was deliberately indifferent to the fact the IRISL and multiple IRISL entities were designated SDNs.

2423. Because Defendants are financial institutions operating in the United States, at all times relevant to the Complaint, each is deemed by law to be aware of all designations made to the SDN list, including without limitation designations for Iran, Hezbollah, al Qaeda, AAI, KAA, the IRGC, the IRGC-QF, Bank Saderat (including Defendant Bank Saderat), Bank Melli, Bank Mellat, Bank Sepah, and IRISL (and multiple IRISL entities).

2424. The Terrorist Attacks constitute acts of international terrorism under 18 U.S.C. § 2331. Further, such acts further constitute "engaging in terrorist activity" under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), and/or "engaging in terrorism" under 22 U.S.C. § 2656f.

2425. At the time each Defendant illegally provided material support to Iran's Agents and Proxies each Defendant also knew or was deliberately indifferent to the fact Iran and its Agents and Proxies, specifically including the Terrorist Groups, all engaged in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, and acts of international terrorism under 18 U.S.C. § 2331 (including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, 2332f, 2339A, 2339B, and/or 2339C), and that Iran provided massive support and sponsorship to its Agents and Proxies for violations of all these statutes, while also providing support for other acts of international terrorism, such as those planned, attempted, and/or perpetrated by the Terrorist Groups, including those designated as FTOs, that resulted in the death or injury to Plaintiffs.

2426. Defendants further knew that such material support would foreseeably facilitate, and indeed did facilitate, acts of international terrorism, terrorist activities, and terrorism, including severe bodily injury, homicides, attempted homicides, or conspiracies to commit homicide against U.S. nationals by Iran and its Agents and Proxies, specifically including the Terrorist Groups, as well as attacks conducted using WMDs, such as EFPs, IEDs, VBIEDs, rockets, and bombs, including attempted bombings, or conspiracies to bomb places of public use, state or government facilities, public transportation systems, or infrastructure facilities which killed or injured Plaintiffs.

2427. As such, at the time it provided material support to Iran's Agents and Proxies, specifically including the Terrorist Groups, each Defendant also knew or was deliberately indifferent to the fact its conduct would foreseeably result in the transfer of at least millions of USDs to known terrorist groups which would then be used to provide material support for terrorist activities (as defined at 8 U.S.C. § (3)(B)(iii)-(iv)), terrorism (as defined at 22 U.S.C. §

2656f), and acts of international terrorism (as defined at 18 U.S.C. § 2331), all of which would be, and ultimately were aimed at U.S. nationals, including Plaintiffs, and Coalition Forces.

2428. In fact, as a result of Defendants' acts: (a) billions of USDs were transferred to known front companies of Iranian-sponsored terrorist organizations, including the NIOC, Mahan Air, Iran Air, Khatam-al Anbiya Construction, IRISL (and multiple IRISL entities), Bank Melli (including Bank Melli plc), Bank Saderat (including Bank Saderat plc), Bank Mellat, Bank Sepah, and Bank Markazi through the United States in a manner designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies; and (b) at least hundreds of millions of USDs were transferred to the Terrorist Groups, who were actively engaged in murdering and maiming U.S. nationals, including Plaintiffs, in Iraq.

2429. At the time Defendants purposefully transferred billions of USD through the United States to known front companies of known terrorist organizations, each Defendant knew that such material support would be delivered to the known terrorist organizations themselves, and the payment order messages facilitating such USD transfers were deliberately and intentionally structured, designed, and processed in a manner expressly devised to ensure that such material support would not be detected, interdicted, or monitored by U.S. regulators and law enforcement agencies.

2430. At the time each Defendant illegally and knowingly provided the material support discussed herein to the known terrorist organizations and the front companies of those terrorist organizations, each Defendant knew, since at least 1984, the United States had formally designated Iran as a State Sponsor of Terrorism subject to various sanctions, and each Defendant further knew, or was deliberately indifferent to the fact, *inter alia*, Iran used its Agents and

Proxies, specifically including at least MOIS, the IRGC, the IRGC-QF, al Qaeda, and Hezbollah, as primary mechanisms to commit, plan, authorize, cultivate, and support terrorism.

2431. Among other things, and as documented by the U.S. State Department, between 2004 and 2011 the IRGC, in concert with Hezbollah, provided training outside of Iraq, as well as sending advisors to Iraq, to assist, train, supply and guide Special Groups and other terrorists in the construction and use of EFPs and other advanced weaponry, devices that constitute “weapons of mass destruction” as defined in 18 U.S.C. § 2332a, incorporating the definition of “destructive devices” set forth in 18 U.S.C. § 924(4)(A)-(C).

2432. Through this clandestine stream of USDs, each Defendant knew, or was deliberately indifferent to the fact, that by providing Iran and its Agents and Proxies with illegal and substantial material support, Defendants foreseeably facilitated the transfer of at least hundreds of millions of USDs to the Terrorist Groups through the international financial system, including payments initiated, processed, altered, modified, falsified, or otherwise released by or through Defendants.

2433. The material support Defendants knowingly and illegally provided to Iran and its Agents and Proxies provided foreseeable and substantial material assistance to the Terrorist Groups. As such, Defendants provided substantial material support to Iran and its Agents and Proxies, specifically including the Terrorist Groups, resulting in violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, 2332d, and/or 2332f, and such conduct proximately caused Plaintiffs’ injuries.

2434. The material support Defendants knowingly and illegally provided to Iran and its Agents and Proxies, specifically including the Terrorist Groups themselves, included, among other things, (1) facilitating at least tens of millions of USDs in illicit transactions on behalf of

MODAFL, the IRGC, Mahan Air, Iran Air, the NIOC, Khatam-al Anbiya Construction, IRISL, Bank Melli (including Bank Melli plc), Bank Saderat (including Bank Saderat plc), Bank Mellat, Bank Sepah, and Bank Markazi, and other instrumentalities of Iranian state-sponsored terror; (2) enabling numerous violations of the U.S. trade embargo against Iran; (3) concealing Iran's efforts to evade U.S. sanctions; and (4) enabling Iran's acquisition from the United States of goods and technologies prohibited by U.S. law to be sold or transferred to Iran, including components of IEDs deployed against U.S. nationals and Coalition Forces in Iraq.

2435. Defendants' intentional and overt acts of purposefully and knowingly providing material support through the provision of expert advice, financial services, and transferring billions of USDs through the United States to Iran and its Agents and Proxies, in a manner expressly designed to ensure the funds could be transferred by and to Iran and its Agents and Proxies without being monitored or interdicted by U.S. regulators and law enforcement agencies, involved and foreseeably led to terrorist acts dangerous to human life, by their nature, and as further evidenced by their consequences. Without the substantial and material assistance provided by Defendants to Iran and its Agents and Proxies, specifically including the Terrorist Groups, could not have carried out the Terrorist Attacks which resulted in Plaintiffs' injuries or deaths.

2436. No Defendant attempted, at any time, to ensure the funds it illegally transferred in violation of U.S. sanctions, would not be transferred to Iran and its Agents and Proxies, including the Terrorist Groups, and used by them to perpetrate acts of international terrorism, including the Terrorist Attacks, that killed or injured Plaintiffs and thousands of other civilians and multinational Coalition Forces.

2437. Each Defendant's purposeful transfers of at least billions of USDs through the United States was done in a manner designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies and foreseeably resulted in material support knowingly being delivered by Defendants to Iran and its Agents and Proxies, including the Terrorist Groups, in order to carry out or prepare for violations of, *inter alia*, 18 U.S.C. §§ 2332(a)-(c), 2332a, and § 2332f, and were thus themselves acts of international terrorism because they were, or objectively appear to have been, intended to: (a) intimidate or coerce the civilian population of the United States and other nations; (b) influence the policy of the governments of the United States and other nations by intimidation or coercion; and/or (c) affect the conduct of the governments of the United States and other nations by facilitating the Terrorist Groups' abilities to prepare for, support, fund, train, initiate, and/or carry out mass destruction and murder of U.S. nationals, including Plaintiffs.

2438. Each Defendant's conduct was a substantial cause in fact and a significant factor in the chain of events leading to Plaintiffs' deaths or injuries, and foreseeably and substantially enhanced the ability of Iran and its Agents and Proxies, including the Terrorist Groups, to engage in terrorist activity (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and/or commit acts of international terrorism (18 U.S.C. § 2331) (including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f and 2339A). Each Defendant's conduct was thus also a substantial and foreseeable cause of Plaintiffs' injuries or deaths.

2439. Furthermore, each Plaintiff's injuries or deaths constitute a harm falling within the foreseeable scope of each Defendant's conduct, as described herein. Injuries and deaths resulting from terrorist attacks (including attacks launched by the Terrorist Groups) that were planned,

supported by, funded, or assisted by Iran are precisely the risks contemplated by Executive Orders, statutes and regulations (including, without limitation, designations under Executive Orders specifically concerning the IRGC, the IRGC-QF, Hezbollah, KAA, Defendant Bank Saderat, and the IRISL) enacted specifically to ensure that Iran had restricted access to USDs and financial services under conditions of maximum transparency, that such USDs were used only for legitimate agencies, operations, and programs and not by or for the benefit of SDNs, and not for Iran's efforts to acquire, develop, and distribute WMDs (including weapons such as EFPs directed at Coalition Forces), and to ensure that any funds Iran did receive that touched U.S. depository institutions could be monitored by U.S. regulators and law enforcement agencies.

2440. Through the conduct as described herein and violating 18 U.S.C. § 2339A in the manner and with the state of mind alleged herein, each Defendant committed acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**B. SECOND CLAIM FOR RELIEF: PRIMARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST COMMERZBANK FOR PROVIDING MATERIAL SUPPORT TO TERRORISTS IN VIOLATION OF 18 U.S.C. § 2339A**

2441. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2442. Defendant Commerzbank provided material support to the IRGC through Commerzbank's acts on behalf of IRISL, and Commerzbank violated § 2339A in concealing and disguising the nature, location, source, and ownership of material support it provided to IRISL, knowing or deliberately indifferent to the fact, that IRISL and the IRGC would use that support in preparation for, or in carrying out acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f .

2443. Defendant Commerzbank knew or was deliberately indifferent to the fact the IRISL was designated an SDN for WMDs-related activities that included arms shipments, including shipments destined for Hezbollah and other terrorists.

2444. The material support that Commerzbank knowingly and illegally provided to the IRISL provided foreseeable and substantial assistance to the IRGC, the IRGC-QF, Hezbollah, AAI, KH, al Qaeda, and the Special Groups, thereby preparing and facilitating acts of terrorism, including the Terrorist Attacks which resulted in the deaths and injuries of Plaintiffs, in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f. Moreover, such material support caused Plaintiffs' deaths and injuries, and thus Commerzbank's conduct was also a substantial and foreseeable cause of Plaintiffs' injuries.

2445. Furthermore, Plaintiffs' injuries and deaths constitute harms falling within the risk contemplated by Commerzbank's material support to the IRGC and IRISL. Injuries resulting from terrorist attacks perpetrated, planned, supported by, funded, or assisted by Iran and Hezbollah are precisely the risks contemplated by statutes and regulations designed to ensure the IRGC, IRISL and Iran had restricted access to USD and financial services, and that any funds they did receive that touched U.S. depository institutions were transparent and could be blocked if warranted, and did not benefit an SDN.

2446. Through the conduct as described herein, by knowingly violating 18 U.S.C. § 2339A in the manner and with the state of mind alleged herein, Commerzbank committed acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**C. THIRD CLAIM FOR RELIEF: PRIMARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST STANDARD CHARTERED BANK FOR PROVIDING MATERIAL SUPPORT TO TERRORISTS IN VIOLATION OF 18 U.S.C. § 2339A**

2447. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2448. Defendant Standard Chartered Bank provided material support to the IRGC and the IRGC-QF through its acts on behalf of Mahan Air, MODAFL and other entities identified *supra* in violation of § 2339A by concealing and disguising the nature, location, source, and ownership of material support it provided to Mahan Air, MODAFL and other entities identified *supra*, knowing or deliberately indifferent to the fact the IRGC and the IRGC-QF would use that material support in preparation for, or in carrying out, acts of international terrorism, including the Terrorist Attacks that resulted in the deaths and injuries of Plaintiffs, and in doing so violated 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f .

2449. Defendant Standard Chartered Bank knew or was deliberately indifferent to the fact Mahan Air, MODAFL and other entities identified *supra* were utilizing Letters of Credit facilitated by Standard Chartered Bank to evade U.S. sanctions and acquire materials used, *inter alia*, to effectuate arms shipments, transport weapons, personnel and technology to the IRGC-QF and Hezbollah.

2450. Mahan Air did, in fact, transport weapons, personnel and technology into Iraq on behalf of the IRGC-QF and Hezbollah and did, in fact, transport modules used to control and activate IEDs and EFPs deployed against Coalition Forces in Iraq.

2451. Iran could not have successfully evaded U.S. sanctions and obtained raw materials and manufacturing equipment prohibited by the International Traffic in Arms Regulations, Export Administration Regulations, and Iran Trade Regulations (“ITRs”) simply by establishing front companies in foreign jurisdictions like Malaysia, Singapore, or Dubai because

those front companies could not have negotiated international payments without being able to provide U.S. and other suppliers with conventional letters of credit drawn on Western banks with established correspondent accounts with U.S. clearing banks.

2452. Nor could the front companies that participated in Iran's clandestine supply chain have succeeded in their efforts had they been forced to rely solely on financing by Iranian banks because those banks could not have provided financing directly because they could not maintain correspondent accounts with U.S. clearing banks and most of them were blacklisted and frozen out of the USD-clearing system.

2453. For example, no legitimate U.S. manufacturer would have agreed to transport materials subject to the International Traffic in Arms Regulations, Export Administration Regulations or ITRs to an unknown company in Singapore or Dubai based on a LC issued by Bank Saderat or Bank Melli.

2454. The linchpin of Iran's illegal and clandestine supply chain was the cooperation of Standard Chartered Bank and the other Defendants who concealed both the role of Iranian banks in providing the credit necessary to finance the transactions and the identities of the Iranian military and IRGC sub-agencies that were actually purchasing the raw materials and manufacturing equipment (invariably being transported to Iran by IRISL, Mahan Air or Iran Air).

2455. With the necessary assistance of Standard Chartered Bank and the other Defendants, MODAFL did in fact acquire spare parts for various military aircraft.

2456. With the necessary assistance of Standard Chartered Bank and the other Defendants, Iranian front companies did purchase hydraulic press components of the kind used

to manufacture EFPs and did purchase steel and copper and other materials necessary for the manufacturing of EFPs and other weapons deployed against Coalition Forces in Iraq.

2457. This substantial and material assistance to Iran's terror apparatus (including the IRGC and MODAFL), knowingly provided by Defendant Standard Chartered Bank, made it possible for Iran to procure the radio frequency modules, metals, and hydraulic presses used to manufacture the copper plates and steel cylinders necessary to manufacture the EFPs and other Iranian weapons used in the attacks on Plaintiffs, as well Iran's transport of weapons, supplies, and IRGC and Hezbollah operatives (who conducted, supervised, and trained the perpetrators of those attacks).

2458. The material support Standard Chartered Bank knowingly and illegally provided to Iran through its Agents and Proxies, including Mahan Air and MODAFL, provided foreseeable and substantial assistance to the IRGC, the IRGC-QF, Hezbollah, al Qaeda, AAI, the Badr Corps/Badr Organization, KH, JAM, the PDB, AAH, Abu Mustafa Al-Sheibani network, Abu Mahdi al-Muhandis network, and/or other terrorist organizations, thereby preparing and facilitating the acts of terrorism that caused Plaintiffs' injuries, all in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f. Thus, Standard Chartered Bank's conduct was also a substantial and foreseeable factor in bringing about Plaintiffs' injuries.

2459. Furthermore, each Plaintiff's injuries and deaths constitute harms falling within the risk contemplated by Standard Chartered Bank's material support to the IRGC, the IRGC-QF, Hezbollah, al Qaeda, AAI, the Badr Corps/Badr Organization, KH, JAM, the PDB, AAH, Abu Mustafa Al-Sheibani network, Abu Mahdi al-Muhandis network, and/or other terrorist organizations. Plaintiffs injuries and deaths resulting from Terrorist Attacks perpetrated, planned,

supported by, funded, or assisted by Iran and its Agents and Proxies, specifically including Hezbollah, are precisely the risks contemplated by statutes and regulations designed to ensure that Iran had restricted access to USDs and financial services, and that any USD funds it did receive that touched U.S. depository institutions were transparent and could be blocked, if warranted, and did not benefit any SDN.

2460. Through the conduct as described herein, by knowingly violating 18 U.S.C. § 2339A in the manner and with the state of mind alleged herein, Standard Chartered Bank committed acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**D. FOURTH CLAIM FOR RELIEF: PRIMARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST COMMERZBANK AG FOR PROVIDING MATERIAL SUPPORT TO HEZBOLLAH IN VIOLATION OF 18 U.S.C. § 2339B**

2461. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2462. Defendant Commerzbank violated § 2339B by providing material support to Hezbollah through Commerzbank's acts on behalf of its customer Waisenkinderprojekt Libanon e.V. (Orphans Project Lebanon e.V.).

2463. Commerzbank knew, or was deliberately indifferent to the fact, that Orphans Project Lebanon e.V. was transferring funds through Commerzbank to FTO Hezbollah and that Hezbollah would use that material support in preparation for, or in carrying out, acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f.

2464. The material support that Commerzbank knowingly and illegally provided to the Orphans Project Lebanon e.V. and hence to Hezbollah, provided foreseeable, substantial assistance to the Hezbollah and the Special Groups, thereby preparing and facilitating acts of

terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus Commerzbank's conduct was also a substantial, foreseeable factor in bringing about Plaintiffs' injuries.

2465. Through the conduct as described herein, by knowingly violating 18 U.S.C. § 2339B in the manner and with the state of mind alleged herein, Commerzbank committed acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**E. FIFTH CLAIM FOR RELIEF: SECONDARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST ALL DEFENDANTS FOR PARTICIPATING IN THE CONSPIRACY**

2466. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein. Defendants entered into the Conspiracy detailed above.

2467. The Terrorist Attacks, which were acts of international terrorism, were within the reasonably foreseeable scope of the Conspiracy. Among other things, it was reasonably foreseeable that the material support Defendants provided in furtherance of the Conspiracy would be used in preparation for and in carrying out said acts of international terrorism.

2468. The Terrorist Attacks were committed, planned, and/or authorized by FTOs, including Hezbollah, al Qaeda and its subgroups, including al Qaeda in Iraq, AAI/Ansar al Sunna, and Kata'ib Hizballah.

2469. Each Defendant's conduct in agreeing to provide Iran and its Agents and Proxies with billions of USDs in an illegal manner, violated 18 U.S.C. § 2339A's express prohibition against concealing or disguising the nature, location, source, or ownership of material support or resources, knowing the material support or resources are to be used in preparation for, or in carrying out, a violation of any of 18 U.S.C. §§ 32, 37, 81, 175, 229, 351, 831, 842(m)-(n), 844(f) or (i), 930 (c), 956, 1091, 1114, 1116, 1203, 1361, 1362, 1363, 1366, 1751, 1992, 2155,

2156, 2280, 2281, 2332, 2332a, 2332b, 2332f, 2340A, or 2442, 42 U.S.C. § 2284, 49 U.S.C. §§ 46502 or 60123 (b), or any offense listed in 18 U.S.C. § 2332b (g)(5)(B) (except for §§ 2339A and 2339B).

2470. The Terrorist Attacks constitute acts of international terrorism under 18 U.S.C. § 2331. Further, the Terrorist Attacks constitute “engaging in terrorist activity” under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv) and/or “engaging in terrorism” under 22 U.S.C. § 2656f.

2471. Defendants, together with other non-defendant co-conspirators (including Iran), agreed to, and did in fact, purposefully transfer billions of USD through the United States knowing that such funds would be delivered to Iran and its Agents and Proxies, specifically including the Terrorist Groups, and the payment order messages facilitating such USD transfers were deliberately and intentionally structured, designed, and processed in a knowing manner expressly meant to ensure that such USD funds would not be detected or monitored by U.S. regulators and law enforcement agencies.

2472. At the time each Defendant illegally provided material support to Iran’s Agents and Proxies, each Defendant knowingly and purposefully agreed to provide such material support and services to Iran and its Agents and Proxies in an illegal manner, knowing or deliberately indifferent to the fact such illegal material support and services furthered Iran’s support for the IRGC, the IRGC-QF, and the Terrorist Groups, and that such agreements and resultant overt acts and conduct would foreseeably, and in fact did, cause acts of international terrorism, terrorist activities, and terrorism, including homicides, attempted homicides, or conspiracies to commit homicide against U.S. nationals, including Plaintiffs by Iran and its Agents and Proxies, as well as attacks conducted with WMDs, such as EFPs, and bombings,

attempted bombings, or conspiracies to bomb places of public use, state or government facilities, public transportation systems, or infrastructure facilities by Iran and its Agents and Proxies.

2473. The material support Defendants knowingly agreed to illegally provide to Iran, as well as its Agents and Proxies, provided foreseeable and substantial assistance to the Iran's Agents and Proxies, specifically including the Terrorist Groups, thereby facilitating and causing the acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' deaths or injuries.

2474. At the time each Defendant illegally provided material support to Iran's Agents and Proxies, specifically including the Terrorist Groups, each Defendant also: (1) knew of the existence of other conspirators, including some or all of the defendants identified herein; and (2) was aware the other conspirators (including the other Defendants and co-conspirators) engaged in the same or similar conduct, and that the other co-conspirators shared the objective of providing material support to Iran and its Agents and Proxies in an illegal manner for the explicit purpose of enabling Iran to avoid U.S. sanctions and regulations enacted specifically to prevent Iran's ability to finance, support, prepare for, plan, or carry out acts of international terrorism by FTOs, including the Terrorist Attacks.

2475. At the time each Defendant illegally provided material support to Iran's Agents and Proxies, each Defendant also knew or was deliberately indifferent to the fact the Conspiracy (a) enabled Iran and its Agents and Proxies to receive USDs from the sale of Iranian oil—money Iran would not otherwise have been able to receive—while the U.S. sanctions and regulations were in place; and (b) prevent U.S. depository institutions, law enforcement, and counter-terrorism agencies from detecting and interdicting Iran's movement of USDs through the global financial system, and thus, each Defendant also knew or was deliberately indifferent to the fact

the overt acts each Defendant performed in furtherance of the Conspiracy facilitated these specific unlawful objectives.

2476. At the time each Defendant illegally provided material support to Iran's Agents and Proxies, each Defendant knew or was deliberately indifferent to the fact the primary purpose of the U.S. sanctions and regulations was to mitigate Iran's sponsorship of terrorism and terrorist organizations (including WMDs proliferation activities in furtherance of such sponsorship), and eliminate or significantly reduce the amount of funds utilized to perpetrate acts of international terrorism, including the massive waves of terrorist attacks launched against U.S. nationals in Iraq.

2477. At the time each Defendant illegally provided material support to Iran's Agents and Proxies, each Defendant knew or was deliberately indifferent to the fact the U.S. sanctions and regulations preventing Iran from receiving USD transfers would be removed if Iran agreed to stop sponsoring terrorism and stop pursuing WMDs.

2478. As a result, at the time each Defendant illegally provided material support to Iran's Agents and Proxies, each Defendant knew or was deliberately indifferent to the fact Iran's primary aim and objective for forming the Conspiracy, and continuing the Conspiracy with each Defendant, was to enable Iran to continue its policy of sponsoring international terrorism, including the Terrorist Attacks, and pursuing WMDs.

2479. At the time each Defendant illegally provided material support to Iran's Agents and Proxies, each Defendant knew or was deliberately indifferent to the fact sponsoring terrorism and pursuing WMDs, was in fact Iran's primary reason for entering into the Conspiracy, and was also Iran's primary objective in continuing the Conspiracy.

2480. As a result, each Defendant knew or was deliberately indifferent to the fact by providing the substantial material resources to Iran and its Agents and Proxies, each Defendant was, in fact, enabling Iran to continue sponsoring international terrorism, including thousands of terrorist attacks against U.S. nationals in Iraq, and pursuing WMDs, and thus, sponsoring international terrorism, themselves. With each successive terrorist group or terrorist act successfully funded, Iran was emboldened to continue the Conspiracy, and continue disregarding the sanctions and regulations imposed by the U.S.

2481. Having entered into an agreement to provide Iran and its Agents and Proxies material support in an unlawful manner, and in direct contravention of U.S. laws and regulations enacted expressly to mitigate Iran's sponsorship of terrorism and terrorist organizations (including WMDs proliferation activities in furtherance of such sponsorship), each Defendant also knew or was deliberately indifferent to the fact, the Conspiracy's aims would foreseeably result in, and in fact did result in, Iran transferring millions of USDs to Hezbollah, AAI, and al Qaeda, all of which were FTOs, as well as other Agents and Proxies of Iran, specifically including the Terrorist Groups, in order to engage in illegal terrorist activities (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism (18 U.S.C. § 2331).

2482. Through the conduct as described herein, by knowingly entering into the Conspiracy in the manner and with the state of mind alleged, it was foreseeable that Iran and its Agents and Proxies would commit, and in fact did commit, the Terrorist Attacks. Thus, each Defendant is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**F. SIXTH CLAIM FOR RELIEF: SECONDARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST COMMERZBANK AG FOR AIDING AND ABETTING HEZBOLLAH, A DESIGNATED FOREIGN TERRORIST ORGANIZATION**

2483. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2484. Defendant Commerzbank aided and abetted Hezbollah, a FTO, by providing material support to Waisenkinderprojekt Libanon e.V. (Orphans Project Lebanon e.V.).

2485. Defendant Commerzbank provided substantial assistance to Orphans Project Lebanon e.V. in an illegal manner, knowing, or deliberately indifferent to the fact, the substantial assistance would be used to provide material support to FTO Hezbollah.

2486. Commerzbank knew, or was deliberately indifferent to the fact, that Orphans Project Lebanon e.V. was transferring funds through Commerzbank to FTO Hezbollah and that Hezbollah would use that material support in preparation for, or in carrying out, acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f.

2487. Commerzbank also aided and abetted Hezbollah by purposefully providing Orphans Project Lebanon e.V. with expert advice and assistance in an illegal manner, knowing or deliberately indifferent to the fact such illegal expert advice and assistance facilitated Orphans Project Lebanon e.V.'s clandestine support for FTO Hezbollah. Commerzbank received highly specialized and technical training and guidance on detecting and preventing the flow of money to terrorists from the government agencies tasked with enforcing the laws. Commerzbank brazenly provided that technical and highly specialized knowledge to Orphans Project Lebanon e.V. as part of their package of illicit financial services knowing, or with deliberate indifference to the fact Orphans Project Lebanon e.V. would use that knowledge to facilitate illegal USD transfers to Hezbollah without being detected by the various enforcement agencies.

2488. Commerzbank's assistance to Hezbollah via Orphans Project Lebanon e.V. was substantial for the following reasons. As a result of the assistance received from Commerzbank, Orphans Project Lebanon e.V. was able to transfer USDs to Hezbollah, despite laws declaring such transfers illegal, despite Hezbollah's designation as a FTO, and despite Commerzbank's legal obligations under the laws of the United States to stop such transfers. As a result of the substantial material support received from Commerzbank, Orphans Project Lebanon e.V. was able to hide their illegal transfers, within a much larger pool of legal USD transfers. As a result of the substantial material support received from Commerzbank, Orphans Project Lebanon e.V. learned how to evade the vast network of tools established by regulators to prevent terrorism. Finally, as a result of the substantial material support received from Commerzbank, Orphans Project Lebanon e.V. was able to achieve their goal of providing material support to Hezbollah for many years while evading detection from authorities.

2489. Commerzbank's substantial material support to Orphans Project Lebanon e.V. was not only substantial because of what each of Commerzbank did for Orphans Project Lebanon e.V., but also substantial because of what Commerzbank did not do, but that Commerzbank was legally required to do. Commerzbank was legally obligated to report to the appropriate authorities, USD transfers to or from FTOs. Instead, Commerzbank remained silent, content with the enormous fees paid to them by Orphans Project Lebanon e.V. for violating U.S. laws, and turning a blind eye to the horrific injuries and loss of life experienced by Plaintiffs and their families in this case.

2490. Commerzbank acted knowingly. As part of the "Know Your Customer" – Anti-Terrorism Act/Bank Secrecy Act laws, Commerzbank had extensive tools and procedures in place to understand their customers, the nature of their customer's business, the laws that apply

to their customers, as well as the risks associated with each of their customers. As bankers, Commerzbank was able to access information about Orphans Project Lebanon e.V. not available to governments or the public. These tools gave Commerzbank an insider's view as to the source and use of Orphans Project Lebanon e.V. funds. Commerzbank knew of the prohibition against transferring funds to FTOs and individuals and entities on the SDN list, and knew of the dangers these individuals and entities represented. Despite this knowledge, Commerzbank agreed to covertly allow Orphans Project Lebanon e.V. to illegally transfer funds to Hezbollah. Commerzbank acted knowingly or with deliberate indifference to the fact the substantial assistance would be used to provide substantial material support to Hezbollah and was deliberately indifferent to the irreparable harm it would cause American peacekeepers.

2491. Commerzbank had a close relationship with Orphans Project Lebanon e.V. that lasted many years. As a result, Orphans Project Lebanon e.V. trusted Commerzbank and Commerzbank trusted Orphans Project Lebanon e.V.

2492. Commerzbank knew, or was deliberately indifferent to the fact, Hezbollah was designated an FTO at all times relevant to this action. Commerzbank also knew Hezbollah engaged in terrorist activities (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism (18 U.S.C. § 2331), including the Terrorist Attacks that resulted in Plaintiffs' deaths or injuries.

2493. The material support that Commerzbank knowingly and illegally provided to the Orphans Project Lebanon e.V. and hence to Hezbollah, provided foreseeable, substantial assistance to the Hezbollah and the Special Groups, thereby preparing and facilitating acts of terrorism, including the Terrorist Attacks that resulted in the deaths and injuries to Plaintiffs, in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, 2332f, 2339A,

2339B, and/or 2339C, and thus, Commerzbank's conduct was also a substantial and foreseeable cause of Plaintiffs' injuries.

2494. Through the conduct as described herein, in the manner and with the state of mind alleged herein, Commerzbank aided and abetted acts of international terrorism, including the Terrorist Attacks, and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**G. SEVENTH CLAIM FOR RELIEF: SECONDARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST ALL DEFENDANTS FOR AIDING AND ABETTING AN ACT OF INTERNATIONAL TERRORISM COMMITTED, PLANNED, OR AUTHORIZED BY DESIGNATED FOREIGN TERRORIST ORGANIZATIONS**

2495. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2496. Defendants knowingly or with deliberate indifference aided and abetted the FTOs—Hezbollah, AAI, KH, and al Qaeda—by illegally facilitating the transfer of billions of USDs through the international financial system to Iran and its Agents and Proxies, knowing or with deliberate indifference to the fact that Iran and its Agents and Proxies would use at least a portion of those funds to provide material support to Hezbollah, AAI, KH, and al Qaeda.

2497. Each Defendant knew, or was deliberately indifferent to the fact, that Iran and its agents and proxies were transferring funds through their correspondent accounts in the U.S. to FTO's, including Hezbollah, Kata'ib Hezbollah, AAI, and al Qaeda, and that those FTO's would use that material support in preparation for, or in carrying out, acts of international terrorism, including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f.

2498. Each Defendant also substantially assisted Iran and its proxies and agents by: (1) purposefully transferring hundreds of billions of USDs through the United States financial

system in a manner expressly designed to purposefully circumvent monitoring by U.S. regulators and law enforcement agencies and evade U.S. sanctions; (2) minimizing the transparency of their illicit financial activities; and (3) purposely providing Iran and its agents and proxies with expert advice and assistance in an illegal manner knowingly, or with deliberate indifference, that their actions would, and in fact did, aid and abet the FTOs by facilitating the transfer of at least tens of millions of USDs in payments to Hezbollah, Kata'ib Hezbollah, AAI, and al Qaeda through the international financial system. In doing so, Defendants were willing to, and did, commit numerous felonies under U.S. law to substantially assist Iran in concealing its financial activities. In doing so, Defendants violated 18 U.S.C. § 2339B by knowingly, or with deliberate indifference, aiding and abetting Hezbollah, al Qaeda, AAI, and KH, all of which were responsible for committing, planning, or authorizing the Terrorist Attacks that caused Plaintiffs' injuries and deaths.

2499. At the time each Defendant illegally provided substantial assistance to Iran's Agents and Proxies, each Defendant also knew or was deliberately indifferent to the fact that providing tens of millions of USDs to Hezbollah, AAI, and al Qaeda, using Defendants' USD clearing services, is squarely within the definition of "material support or resources" contemplated by Congress when enacting 18 U.S.C. § 2339B, and violates Congress' stated goal of cutting off the flow of money to terrorists. Congress defined "Material support or resources" in 18 U.S.C. § 2339 to include "...any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services,..."

2500. Defendants also aided and abetted Hezbollah, al Qaeda, AAI, and KH by purposefully providing Iran and its Agents and Proxies with expert advice and assistance in an illegal manner, knowing or deliberately indifferent to the fact such illegal expert advice and

assistance facilitated Iran's support for the FTOs that carried out the Terrorist Attacks which resulted in Plaintiffs' injuries or deaths. Congress defined material support or resources to include "expert advice or assistance" which is defined in 18 U.S.C. § 2339 to include "advice or assistance derived from ...technical or other specialized knowledge." Defendants each received extensive training and guidance on detecting and preventing the flow of money to terrorists from the government agencies tasked with enforcing the laws. Defendants brazenly provided that technical and highly specialized knowledge to Iran and its Agents and Proxies, as part of their package of illicit financial services knowing or with deliberate indifference to the fact Iran and its Agents and Proxies would use that specialized and highly technical knowledge to conduct at least tens of millions of illegal USD transfers, to Hezbollah, al Qaeda, AAI, and KH without being detected by the various enforcement agencies.

2501. As a result of the assistance received from each Defendant, (1) Iran and its Agents and Proxies were able to transfer USDs to and from any party, at any time, regardless of the laws declaring such transfers illegal, regardless of whether the recipient was a FTO, and regardless of any particular Defendant's legal obligations under the laws of the United States to stop such transfers; (2) Iran was able to hide billions of USDs in illegal transfers within a much larger pool of legal USD transfers; (3) the economic sanctions against Iran, which were aimed at stopping Iran from sponsoring terrorism, were ineffective; (4) Iran learned how to evade the vast network of tools established by regulators to prevent terrorism; and (5) Iran was able to achieve its goal of providing substantial and material support to Hezbollah, al Qaeda, AAI, and KH, including the FTOs responsible for carrying out the attacks which killed or injured Plaintiffs, all while evading detection from authorities. Thus, Defendant's assistance to Iran and its Agents and Proxies was substantial for at least the aforementioned reasons, and such substantial assistance provided to

Iran and its Agents and Proxies aided and abetted Hezbollah, al Qaeda, AAI, and KH by, among other things, providing those FTOs with material support which, in turn, they used to plan, authorize, train for, and conduct their terrorist activities, including the Terrorist Attacks.

2502. Defendants' assistance to Iran was not only substantial because of what each Defendant did for Iran, but also substantial because of what each Defendant did not do, but were legally required to do. Each Defendant was legally obligated to report to the authorities, transfers to or from FTOs. Instead, each Defendant remained silent, content with the enormous fees paid to it by Iran for violating U.S. laws and turning a blind eye to the horrific injuries and loss of life experienced by Plaintiffs and their families in this case.

2503. The assistance provided by each Defendant to Iran was essential for Iran. Defendants illegally allowed Iran access to the U.S. financial system, the largest USD clearing system in the world. There is no alternative financial system capable of transferring the hundreds of billions of USDs around the world that Iran required. Alternative methods such as black market exchanges, bulk cash smugglers, and third party intermediaries, are not only unsafe and inefficient, but they do not have the collective ability to transfer the hundreds of billions of USDs required by Iran. Perhaps even more importantly, unlike the cartels whose business is conducted in "cash," proceeds from oil sales are transferred electronically. As a result, it was essential for Iran to obtain the unlawful assistance from Defendants who, in the course of their normal business activities, each transfer billions of USDs electronically each day.

2504. Additionally, the banks acted knowingly. As part of the "Know Your Customer" – Anti-Terrorism Act / Bank Secrecy Act laws, each Defendant had extensive tools and procedures in place to understand their customer, the nature of their customer's business, the laws that apply to their customers, as well as the risks associated with each of their customers. Defendants were

able to access information about their customers not available to governments or the public. These tools gave Defendants an insider's view as to the source and use of their customer's funds. Each of the banks knew of the prohibition against transferring funds to people/entities on the SDN list, and knew of the dangers these individuals/entities represented. Despite this knowledge, each Defendant agreed to transfer funds covertly and illegally to and from entities, including FTOs, listed on the SDN list, on behalf of Iran. Each of the defendants knew of the sanctions in place against Iran, knew the reason those sanctions were implemented, and knew the types of transactions they were performing on behalf of Iran were illegal, but performed them anyway. The banks acted knowingly or with deliberate indifference to the fact the substantial assistance would be used to provide material support to Hezbollah, AAI, Kata'ib Hezbollah and al Qaeda, and were deliberately indifferent to the irreparable harm that it would cause American peacekeepers and other U.S. nationals.

2505. Each Defendant had a close relationship with Iran that lasted many years. In fact, for many of the defendants, Iran had been a client for many years prior to the start of the Conspiracy. As a result, Iran trusted Defendants and Defendants trusted Iran. Iran trusted Defendants to clear hundreds of millions of USDs each day, in oil sale proceeds, in violation of international sanctions. Iran trusted Defendants to not disclose to authorities their illegal transfers of USDs to FTOs.

2506. While each Defendant was providing Iran and its Agents and Proxies with substantial assistance in an unlawful manner knowing, or deliberately indifferent to the fact it would be used to aid and abet Hezbollah, AAI, KH, and al Qaeda, each Defendant also knew Iran had, since 1984, been officially designated by the United States as a State Sponsor of Terrorism, subject to numerous U.S. sanctions, and knew or was deliberately indifferent to the

fact such designation was based in part on Iran's sponsorship and patronage of Hezbollah, AAI, al Qaeda, and other FTOs (specifically including the FTOs responsible for carrying out the Terrorist Attacks which killed or injured Plaintiffs), and that Iran used Hezbollah as a primary mechanism to enable it to cultivate and support terrorism.

2507. Each Defendant knew, or was deliberately indifferent to the fact, Hezbollah and al Qaeda, were designated FTOs at all times relevant to this action, and that KH was designated a FTO in 2009. Each Defendant also knew that Hezbollah, AAI, and al Qaeda engaged in terrorist activities (8 U.S.C. § 1182(a)(3)(B)(iii)-(iv)), terrorism (22 U.S.C. § 2656f), and acts of international terrorism (18 U.S.C. § 2331).

2508. The acts of international terrorism that injured or killed Plaintiffs constitute acts of international terrorism under 18 U.S.C. § 2331, and constitute "engaging in terrorist activity" under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), and/or "engaging in terrorism" under 22 U.S.C. § 2656f.

2509. The substantial assistance each Defendant provided to Iran and its Agents and Proxies, knowingly or with deliberate indifference to the fact it would be, and in fact was, used to aid and abet Hezbollah, AAI, KH, and al Qaeda, constituted material support to Hezbollah, al Qaeda, AAI, and KH and facilitated acts of terrorism, including the Terrorist Attacks, in violation of §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f.

2510. Without such material support, Hezbollah, AAI, KH, and al Qaeda could not have carried out the Terrorist Attacks which resulted in Plaintiffs' injuries or deaths.

2511. Through its conduct as described above, by knowingly providing substantial assistance to Iran and its Agents and Proxies in an unlawful manner, and knowingly or deliberately indifferent to the fact the substantial assistance would be used to provide material

support to FTOs, including Hezbollah, Kata'ib Hezbollah, AAI, and al Qaeda, each Defendant is liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

2512. Through the conduct as described herein, each Defendant aided and abetted Iran and its Agents and Proxies to commit acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**H. EIGHTH CLAIM FOR RELIEF: PRIMARY LIABILITY AGAINST HSBC BANK USA, N.A. UNDER 18 U.S.C. § 2333(A) FOR ENGAGING IN FINANCIAL TRANSACTIONS WITH IRAN IN VIOLATION OF 18 U.S.C. § 2332D**

2513. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2514. As alleged above, at all relevant times HSBC-US knew Iran was a country designated by the United States under section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. § 2405) as a country supporting international terrorism, yet HSBC-US nevertheless engaged in thousands of financial transactions with Iran in violation of 18 U.S.C. § 2332d.

2515. Pursuant to 31 C.F.R. § 560.304, Bank Markazi, Bank Sepah, Bank Melli Iran, and the NIOC constitute the government of Iran.

2516. Defendant HSBC-US is a juridical person organized under the laws of the United States pursuant to 18 U.S.C. § 2332d(b)(2)(C), and is also a person within the United States pursuant to 18 U.S.C. § 2332d(b)(2)(D).

2517. Pursuant to 18 USC 2331 (3) the term “person” means any individual or entity capable of holding a legal or beneficial interest in property.

2518. Each Defendant held a legal or beneficial interest in property in the U.S. during the relevant period and as such qualified as a “person in the United States” for purposes of 18 U.S.C. § 2332d(b)(2)(D).

2519. Defendant HSBC-US knew, or was deliberately indifferent to the fact, that Hezbollah had been designated an FTO.

2520. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, that AAI and al Qaeda were designated as FTOs.

2521. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, the IRGC-QF had been designated an SDGT.

2522. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, that Bank Saderat (including Defendant Bank Saderat) had been designated an SDGT.

2523. Defendant HSBC-US also knew, or was deliberately indifferent to the fact, the IRGC and KAA had been designated as SDNs.

2524. Defendant HSBC-US also knew or was deliberately indifferent to the fact the IRISL and multiple IRISL entities had been designated SDNs.

2525. As set forth above, HSBC-US knowingly conducted illegal financial transactions on behalf of Iran through Bank Melli and other Iranian counter-parties that did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department – regulations passed for the specific purposes of mitigating the risk that funds transfers to Iran could be used to: engage in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, or acts of international terrorism under 18 U.S.C. § 2331.

2526. In fact, the transactions at issue (including at least the \$183 million HSBC-US facilitated on behalf of sanctioned entities in Iran that were identified in HSBC-US's December 11, 2012 DPA with DOJ) explicitly violated 31 C.F.R 535.701(a)(2) and 31 C.F.R 560.203.

2527. Defendant HSBC-US knew that Defendants HSBC-Europe and HBME were deliberately altering and omitting information in funds transfer payment order messages being

processed through HSBC-US, thereby evading U.S. laws and regulations whose express purpose was (and is) to ensure that only a very limited class of payments could be facilitated to Iran, and that payment order messages for such funds transfers required transparency in order to ensure the transfers qualified for the limited exceptions and exemptions and did not result in U.S. depository institutions processing transactions for the benefit of SDNs.

2528. As set forth in detail above, throughout the Relevant Period, HSBC-US knew that other HSBC Defendants (such as HSBC-London and HBME) were providing material support to Iran in a manner violative of U.S. laws and regulations, and HSBC-US also knew its own systems and networks were being used to unlawfully facilitate the HSBC Defendants' illegal conduct.

2529. Defendant HSBC-US also knew or was deliberately indifferent to the fact Iran and its Agents and Proxies, the IRGC, IRISL, Hezbollah, and Defendant Bank Saderat all engaged in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, and acts of international terrorism under 18 U.S.C. § 2331 (including violations of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f), and that Iran provided massive support and sponsorship for violations of all these statutes, while also providing support for other acts of international terrorism, such as those planned, attempted, and/or perpetrated by the Terrorist Groups.

2530. Knowing Defendants HSBC-London and HBME were moving billions of sanction-evading Iranian USDs through HSBC-US's offices with the specific intent of defeating HSBC-US's OFAC filters and violating HSBC-US reporting requirements, it was foreseeable that HSBC-US's conduct would provide substantial and material support to Iran and its Agents and Proxies, (specifically including Hezbollah, the IRGC, the IRGC-QF, AAI, al Qaeda, the

Special Groups, and the Terrorist Groups) to engage in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, and acts of international terrorism under 18 U.S.C. § 2331, including the Terrorist Attacks which resulted in Plaintiffs' injuries and deaths.

2531. Defendant HSBC-US's conduct foreseeably and substantially enhanced Hezbollah's, the IRGC's, the IRGC-QF's, AAI's, al Qaeda's, the Special Groups', the Terrorist Groups, and other Iranian-sponsored terrorists' ability to engage in terrorist activity, including preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries and deaths, and thus HSBC-US's conduct was also a substantial and foreseeable cause of Plaintiffs' injuries and deaths.

2532. Through the conduct as described herein, by knowingly violating 18 U.S.C. § 2332d in the manner and with the state of mind alleged herein, HSBC-US committed acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**I. NINTH CLAIM FOR RELIEF: PRIMARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST STANDARD CHARTERED BANK, ROYAL BANK OF SCOTLAND N.V., COMMERZBANK, DEUTSCHE BANK AG, BARCLAYS BANK PLC, AND CREDIT SUISSE, FOR ENGAGING IN FINANCIAL TRANSACTIONS WITH IRAN AND ITS AGENTS AND PROXIES IN VIOLATION OF 18 U.S.C. § 2332D**

2533. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2534. Defendants SCB, ABN AMRO (RBS N.V.), Commerzbank, DB, Barclays, and Credit Suisse each utilized their respective New York branches in connection with their agreement to provide Iran material support in an illegal manner in order to effectuate and

facilitate the Conspiracy, and each of those respective New York branches is a “person in the United States” within the scope of 18 U.S.C. § 2332d(b)(2)(D).

2535. Pursuant to 18 USC 2331 (3) the term “person” means any individual or entity capable of holding a legal or beneficial interest in property.

2536. Each Defendant held a legal or beneficial interest in property in the U.S. during the relevant period and as such qualified as a “person in the United States for purposes of 18 U.S.C. § 2332d(b)(2)(D).

2537. Each Defendant knew or was deliberately indifferent to the fact Iran was designated under section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. § 2405) as a country supporting international terrorism and nonetheless knowingly engaged in thousands of illegal financial transactions with the government of Iran through their U.S. operations.

2538. Pursuant to 31 C.F.R. § 560.304, Bank Markazi, Bank Sepah, Bank Melli Iran, and the NIOC constitute the government of Iran.

2539. The New York branch of each of the above-referenced Defendants also knew, or was deliberately indifferent to the fact, that Hezbollah, AAI, KH, and al Qaeda had been designated as FTOs, the IRGC-QF and Bank Saderat (including Defendant Bank Saderat) had each been designated an SDGT, and that multiple other Iranian Agents and Proxies (including the IRGC, Bank Melli, Bank Mellat, Bank Sepah, KAA, IRISL (and multiple IRISL entities)) had been designated SDNs.

2540. The New York branches of the above-referenced Defendants also knew or were deliberately indifferent to the fact Bank Melli (including Melli Bank Plc), Bank Saderat (including Defendant Bank Saderat), Bank Mellat, and Bank Sepah had been designated SDNs

before November 2008, and, as such, were excluded from accessing the U-Turn exemption in the Iranian Transaction Regulations.

2541. As set forth above, the illegal transactions knowingly facilitated through New York by the respective New York branches of the above-referenced Defendants thus did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department for U-Turn exemption transactions, and therefore violated the criminal provisions of 18 U.S.C. § 2332d(a).

2542. In fact, the transactions at issue (including the billions of dollars facilitated on behalf of sanctioned entities in Iran that were identified in each Defendant's DPA's with the DOJ and in the Settlement Agreements with the NYDFS) explicitly violated 31 C.F.R 535.701(a)(2) and 31 C.F.R 560.203.

2543. Each of the above-referenced Defendants' New York branch's acts transcended national boundaries in terms of the means by which they were accomplished.

2544. Each of the above-referenced Defendants' New York branch's conduct foreseeably and substantially enhanced Hezbollah's, AAI's, KH's, al Qaeda's, the IRGC's and the Terrorist Groups' and other Iranian sponsored terrorists' ability to engage in terrorist activity, including preparing and facilitating acts of terrorism in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f that caused Plaintiffs' injuries, and thus each of the above Defendants' New York branch's conduct was also a substantial, foreseeable factor in bringing about Plaintiffs' injuries.

2545. The New York branches of each of the above-referenced Defendant's knowingly, or with deliberate indifference provided unlawful financial services to Iran in the United States, knowing that its conduct was unlawful and enabled Iran to move millions (or in some cases,

billions) of USDs through the United States' financial system without those funds being monitored or detected by U.S. regulators and law enforcement agencies. That conduct involved acts that were necessarily dangerous to human life, by their nature and as evidenced by their consequences.

2546. Furthermore, each Plaintiff's injuries or death constitute a harm falling within the risk contemplated by each of the above-referenced Defendants' New York branch's knowing and unlawful conduct, including their knowledge or deliberate indifference to the full scope, objectives, and results of their actions. The injuries or deaths of Plaintiffs resulting from terrorist attacks (including attacks launched by the IRGC, the IRGC-QF, Hezbollah, al Qaeda, AAI, the Badr Corps/Badr Organization, KH, JAM, the PDB, AAH, Abu Mustafa al-Sheibani network, Abu Mahdi al-Muhandis network, and/or other terrorist organizations (including the Special Groups)) are precisely the risks contemplated by Executive Orders, statutes and regulations (including, without limitation, designations under Executive Orders specifically concerning the IRGC, KAA, Defendant Bank Saderat, and the IRISL) enacted specifically to ensure that such organizations either have no access, or restricted access to USD and financial services under conditions of maximum transparency, such that USDs will be used only for legitimate operations and programs and not by or for the benefit of terrorist organizations, and to ensure that any funds that touched U.S. depository institutions could be monitored by U.S. regulators and law enforcement agencies.

2547. Each of the above-referenced Defendants' criminal violations of the provisions of 18 U.S.C. § 2332d(a) was a substantial cause of Plaintiffs' injuries and deaths, and, for the reasons set forth herein, constitutes an act of international terrorism rendering each of the above Defendants liable for damages to each Plaintiff for their injuries pursuant to 18 U.S.C. § 2333(a).

2548. Through the conduct as described herein, by knowingly violating 18 U.S.C. § 2332d in the manner and with the state of mind alleged herein, SCB, ABN AMRO (RBS N.V.), Commerzbank, DB, Barclays, and Credit Suisse committed acts of international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**J. TENTH CLAIM FOR RELIEF: PRIMARY LIABILITY UNDER 18 U.S.C. § 2333(A) AGAINST BNP FOR ENGAGING IN FINANCIAL TRANSACTIONS WITH IRAN AND SUDAN AND THEIR AGENTS AND PROXIES IN VIOLATION OF 18 U.S.C. § 2332D**

2549. Plaintiffs repeat and re-allege each and every allegation of the foregoing paragraphs as if fully set forth herein.

2550. Defendants BNP utilized its New York branch to engage in financial transactions with Iran and Sudan, and BNP's New York branch is a "person in the United States" within the scope of 18 U.S.C. § 2332d(b)(2)(D).

2551. Pursuant to 18 USC 2331 (3) the term "person" means any individual or entity capable of holding a legal or beneficial interest in property.

2552. BNP held a legal or beneficial interest in property in the U.S. during the relevant period and as such qualified as a "person in the United States for purposes of 18 U.S.C. § 2332d(b)(2)(D).

2553. As set forth above, BNP knew or was deliberately indifferent to the fact Iran and Sudan were each designated under section 6(j) of the Export Administration Act of 1979 (50 App. U.S.C. § 2405) as a country supporting international terrorism and nonetheless knowingly engaged in thousands of illegal financial transactions with the governments of Iran and Sudan through their U.S. operations in violation of 18 U.S.C. § 2332d.

2554. Pursuant to 31 C.F.R. § 560.304, Bank Markazi, Bank Sepah, Bank Melli Iran, and the NIOC constitute the government of Iran.

2555. Pursuant to 31 C.F.R. § 560.305, the Central Bank of Sudan constitutes the government of Sudan.

2556. BNP knew, or was deliberately indifferent to the fact, that Hezbollah, AAI, and al Qaeda all were designated as FTOs, the IRGC-QF and Bank Saderat (including Defendant Bank Saderat) were designated as SDGTs, and that multiple other Iranian Agents and Proxies (including the IRGC, Bank Melli, Bank Mellat, Bank Sepah, NIOC, KAA, and IRISL (and multiple IRISL entities)) had been designated SDNs.

2557. As set forth above, the illegal transactions knowingly facilitated through New York by BNP thus did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department for U-Turn exemption transactions, and therefore violated the criminal provisions of 18 U.S.C. § 2332d(a). In fact, the transactions at issue explicitly violated 31 C.F.R 535.701(a)(2) and 31 C.F.R 560.203.

2558. BNP knew, or was deliberately indifferent to the fact, that Usama bin Ladan was a major shareholder of Bank al Shamal, and that his brother-in-law, himself a designated terrorist and terrorist financier, was Chairman of Bank al Shamal, and that Bank al Shamal funded al Qaeda operations with US dollars.

2559. As set forth above, the illegal transactions knowingly facilitated through New York by BNP thus did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department for U-Turn exemption transactions, and therefore violated the criminal provisions of 18 U.S.C. § 2332d(a). In fact, the transactions at issue explicitly violated 31 C.F.R 538.701(a)(2).

2560. OFAC has identified the NIOC as being owned or controlled by the Government of Iran.

2561. As set forth above, BNP knowingly conducted illegal financial transactions on behalf of a client, identified in the DOJ statement of facts as “Iranian Controlled Company 1.” The payments were in connection with three letters of credit that facilitated the provision of liquefied petroleum gas to an entity in Iraq.

2562. BNP’s “Know Your Customer” documentation on Iranian Controlled Company 1” showed it was 100% owned by Iranian Energy Group 1. BNP’s documentation also showed that Iranian Energy Group 1, and in turn Iranian Controlled Company 1, was 100% owned by an Iranian citizen.

2563. BNP knowingly, intentionally and willfully processed a total of approximately \$586.1 million in transactions with Iranian Controlled Company 1, in violation of U.S. sanctions against Iran.

2564. As set forth herein, BNP knowingly conducted illegal financial transactions on behalf of Iran through Iranian counter-parties that did not fall within the safe harbor provisions of the regulations issued by the U.S. Treasury Department – regulations passed for the specific purposes of mitigating the risk that funds transfers to Iran could be used to: engage in terrorist activity under 8 U.S.C. § 1182(a)(3)(B)(iii)-(iv), terrorism under 22 U.S.C. § 2656f, or acts of international terrorism under 18 U.S.C. § 2331.

2565. In fact, the transactions at issue (including approximately \$100.5 million in U.S. dollar payments involving an Iranian oil company following the revocation of the U-Turn Exemption, were identified in BNP’s June 28, 2014 Statement of Facts with DOJ) explicitly violated 31 C.F.R 535.701(a)(2) and 31 C.F.R 560.203. These payments were in connection with six letters of credit issued by BNP that financed Iranian petroleum and oil exports – and the payments were made even after compliance personnel at BNP Paribas Paris alerted ECEP

employees the USD payments associated with these letters of credit “are no longer allowed by American authorities.”

2566. Defendant BNP deliberately altered and omitted information in funds transfer payment order messages being processed through BNP, thereby evading U.S. laws and regulations whose express purpose was (and is) to ensure that only a very limited class of payments could be facilitated to Iran, and that payment order messages for such funds transfers required transparency in order to ensure the transfers qualified for the limited exceptions and exemptions, and did not result in U.S. depository institutions processing transactions for the benefit of SDNs.

2567. BNP’s conduct foreseeably and substantially enhanced the Terrorist Group’s (including without limitation Hezbollah’s, AAI’s, al Qaeda’s, KH’s, the IRGC’s, the IRGC-QF’s, and other Iranian sponsored terrorists’ ability to engage in terrorist activity, including preparing and facilitating acts of terrorism, including the Terrorist Attacks that resulted in Plaintiffs’ deaths and injuries, in violation of 18 U.S.C. §§ 1114, 1203, 1362, 2332(a), 2332(b), 2332(c), 2332a, and/or 2332f, and thus BNP’s conduct was also a substantial and foreseeable cause of Plaintiffs’ injuries.

2568. BNP’s criminal violations of the provisions of 18 U.S.C. § 2332d(a) was a substantial cause of Plaintiffs’ injuries, and, for the reasons set forth herein, constitute acts of international terrorism rendering BNP liable for damages to Plaintiffs for their injuries and deaths pursuant to 18 U.S.C. § 2333(a).

2569. Through the conduct as described herein, by knowingly violating 18 U.S.C. § 2332d in the manner and with the state of mind alleged herein, BNP committed acts of

international terrorism and is liable for damages to Plaintiffs for their respective injuries or deaths pursuant to 18 U.S.C. § 2333(a).

**X. PRAYER FOR RELIEF**

**WHEREFORE**, Plaintiffs demand:

- a) Judgment for all Plaintiffs against Defendants for compensatory damages, including, but not limited to, physical injury, physical and mental pain and suffering, loss of enjoyment of life, medical expenses, lost income, lost earning capacity, loss of services, loss of solatium, and loss of consortium in amounts to be determined at trial;
- b) Judgment for Plaintiff Estates against Defendants for compensatory damages for the extrajudicial killing of the decedents, including, but not limited to, physical injury, mental anguish, pain and suffering, loss of consortium, loss of support, loss of services, and all other pecuniary loss, including funeral expenses, medical expenses, loss of earnings, loss of income, and loss of net accumulations to the estates, in amounts to be determined at trial;
- c) Judgment for all Plaintiffs against Defendants for treble damages, costs, and attorney's fees pursuant to 18 U.S.C. § 2333(a);
- d) Interest; and
- e) Such other and further relief as the Court finds just and equitable.

**PLAINTIFFS DEMAND A JURY TRIAL ON ALL THE ISSUES SO TRIABLE.**

Respectfully Submitted,

Dated: November 9, 2017

**BURG, SIMPSON, ELDREDGE, HERSH  
AND JARDINE, P.C.**

By: /s/ Seth Katz

Seth Katz  
SDNY Bar No. SK4518  
40 Inverness Drive East  
Englewood, Colorado 80112  
Telephone: 303.792.5595  
Facsimile: 303.708.0527  
Email: skatz@burgsimpson.com

**MM~LAW LLC**

Gavriel Mairone (*Pro Hac Vice* to be filed)  
Illinois Bar No. 618698  
Bena Ochs  
SDNY Bar No. BO1602  
980 North Michigan Avenue, Suite 1400  
Chicago IL 60611  
Telephone: 312.253.7444  
Facsimile: 312.275.8590  
Email: [ctlaw@mm-law.com](mailto:ctlaw@mm-law.com)  
[bena@mm-law.com](mailto:bena@mm-law.com)

**LEVIN, PAPANTONIO, THOMAS, MITCHELL,  
RAFFERTY AND PROCTOR, P.A.**

Troy A. Rafferty (*Pro Hac Vice* to be filed)  
Florida Bar No. 24120  
Christopher G. Paulos (*Pro Hac Vice* to be filed)  
Florida Bar No. 0091579  
Jeffrey Gaddy (*Pro Hac Vice* to be filed)  
Florida Bar No. 53046  
Troy Bouk (*Pro Hac Vice* to be filed)  
Florida Bar No. 43384  
316 South Baylen Street, Suite 600  
Pensacola, Florida 32502  
Telephone: 850.435.7000  
Facsimile: 850.436.6123  
Email: [trafferty@levinlaw.com](mailto:trafferty@levinlaw.com)  
[cpaulos@levinlaw.com](mailto:cpaulos@levinlaw.com)  
[jgaddy@levinlaw.com](mailto:jgaddy@levinlaw.com)  
[tbouk@levinlaw.com](mailto:tbouk@levinlaw.com)

**LUCAS MAGAZINE**

James L. Magazine (*Pro Hac Vice* to be filed)  
Florida Bar No. 0847232  
8606 Government Drive  
New Port Richey, Florida 34654  
Telephone: 727.849.5353  
Facsimile: 727.845.7949  
Email: [jim@lucasmagazine.com](mailto:jim@lucasmagazine.com)

Michael B. Angelovich (*Pro Hac Vice* to be filed)  
Texas Bar No. 00785666  
Chad E. Ihrig (*Pro Hac Vice* to be filed)  
Texas Bar No. 24084373  
Christian Hurt (*Pro Hac Vice* to be filed)  
Texas Bar No. 24059987  
3600 N. Capital of Texas Highway  
Building B, Suite 350  
Austin, Texas 78746  
Telephone: 512.328.5333  
Facsimile: 512.328.5335  
Email: [mangelovich@nixlaw.com](mailto:mangelovich@nixlaw.com)  
[cihrig@nixlaw.com](mailto:cihrig@nixlaw.com)  
[christianhurt@nixlaw.com](mailto:christianhurt@nixlaw.com)

**THE NATIONS LAW FIRM**

Howard L. Nations  
SDNY Bar No. HN4663  
Rachel V. Rose (*Pro Hac Vice* to be filed)  
Texas Bar No. 24074982  
3131 Briarpark Drive, Suite 208  
Houston, Texas 77042  
Telephone: 713.807.8400  
Facsimile: 713.807.8423  
Email: [rachel.rose@howardnations.com](mailto:rachel.rose@howardnations.com)  
[howard@howardnations.com](mailto:howard@howardnations.com)

**SPANGENBERG, SHIBLEY, AND LIBER LLP**

William Hawal (*Pro Hac Vice* to be filed)

Ohio Bar No. 0006730

Jeremy Tor

SDNY Bar No. JT8165

1001 Lakeside Avenue E, No. 1700

Cleveland, Ohio 44114

Telephone: 216.600.0114

Facsimile: 216.696.3924

Email: whawal@spanglaw.com

jtor@spanglaw.com

*Counsel for Plaintiffs*